National Aeronautics and Space Administration

A Product of the

NASA SAFETY CENTER &

OFFICE OF THE CHIEF KNOWLEDGE OFFICER, GODDARD SPACE FLIGHT CENTER

Selected NASA
CASE STUDIES

February 2009

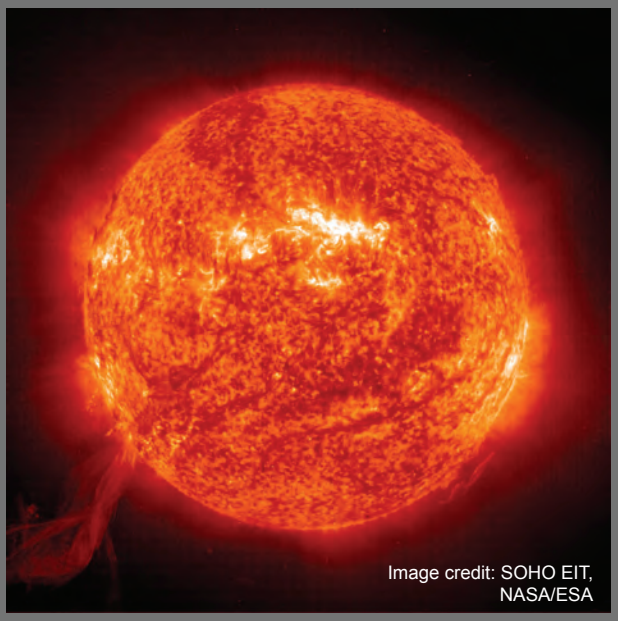


Image credit: SOHO EIT, NASA/ESA

An image of the sun captured by the Solar and Heliospheric Observatory (SOHO) Extreme Ultraviolet Imaging Telescope (EIT) on 10/25/2002. Read about how SOHO was lost and miraculously recovered in "Million Mile Rescue," pages 34-37.

Image credit: NASA/JHU APL

An artist's conception of STEREO's two observatories opening their solar panels. Read about the challenges of developing the Solar Terrestrial Relations Observatory (STEREO) in "STEREO: Organizational Cultures in Conflict," pages 14-23.

Image credit: NASA

The Atlas Centaur-68 launch vehicle with the FLTSATCOM F-8 communication satellite aboard, on Complex 36 at Cape Canaveral Air Force Station, 9/25/1990. Study the launch of AC-67 with the FLSATCOM F-6 satellite in "Atlas Centaur-67: Go or No Go for Launch?" pages 24-26.

Table of Contents

Welcome

As an Agency, we at NASA desire to be a learning organization, to capture and apply the knowledge we have acquired through years of exploration and innovation. The NASA Safety Center and the Office of the Chief Knowledge Officer at Goddard Space Flight Center collaborated to bring you this collection of NASA case studies, because we believe open communication and thoughtful conversation promote mission success. The case studies in this collection use our history to help us continue moving past the limits of familiar human experience.

The rationale for the case method is that organizations learn most effectively when knowledge is shared in usable ways among organization members, and that knowledge is most useful when it is contextual—when it relates to personal experience. Inert information databases, such as a lessons-learned system, may be part of a knowledge-management process, but by themselves they are insufficient for creating dynamic organizational learning. The case study, on the other hand, builds a learning context and fosters the systems-thinking skills a learning organization needs.

Some cases are meant to be read individually, to stimulate reflection. Others make for good short discussions in staff meetings, warm-up exercises at team meetings or other training events. Many of the case studies that follow can provide the basis for intensive workshops or for shorter exercises that focus on only one of several topics.

This collection includes three types of NASA case studies, each with a unique focus and story-telling approach. Decision-Oriented Case Studies emphasize the decision-making process, System Failure Case Studies concentrate on understanding the complex causes of system-wide catastrophes, and Cases of Interest use real-life events to highlight issues that are often overlooked in the day-to-day business of managing our missions.

As we share these stories, we must accept some risk of causing offense. The alternative is a certain repetition of mistakes that we as a global community cannot afford to make if we are to succeed in this business of exploring our world and the universe beyond. This collection is intended to help those both within and outside of NASA benefit and learn from our experience managing and executing our missions.

The most important thing to remember is that the case is a tool to generate conversation and thinking. It is a sharpening tool; in the end, the people who engage in the case are sharper and better equipped for the tasks lying ahead of them. Use these cases, download others, and learn to generate your own. You'll find an amazing response to the real learning opportunities they create as people engage and share their own lessons learned.

Sincerely,

Alan Phillips,
Director
NASA Safety Center

Edward Rogers,
Chief Knowledge Officer
Goddard Space Flight Center

WHAT IS A Case Study?

A case study may be understood best as simply a tool for creating an opportunity for conversation. It is a story, told in narrative form and based on actual events. An effective case study transfers specific knowledge and learning by placing participants in a position to think through real-life choices that confronted decision-makers. The element of realism helps participants in the learning process develop analytical techniques they can draw upon when faced with similar choices in their own projects; the narrative context provides a concrete base for practical lessons from the story.

CASE STUDIES IN THIS COLLECTION

Decision-Oriented Case Studies, the type developed and used at Goddard, are structured and written from the viewpoint of a key player. They are framed around information available to the protagonist at the time of the event (so the reader doesn't have the benefit of hindsight). The case typically builds to a point where the decision-maker is confronted with open-ended choices, then leaves the reader to analyze the information and make critical decisions based on contextual analysis.

System Failure Case Studies, on the other hand, use the clarity of hindsight to help participants recognize and prevent potential future disasters. The NASA Safety Center's System Failure Case Studies examine catastrophic failures and the systemic weaknesses that contributed to them. While participants do discuss decision-making processes in these case studies, they focus on developing a better understanding of how small, seemingly insignificant problems can combine into dramatic failures. After working through a case study, participants will better understand complex systems, know how to recognize warning signs and system weaknesses, and be prepared to mitigate systemic hazards.

Cases of Interest are short, two-page case studies, produced at the NSC, that are narrower in scope and tend to be fairly straightforward. While both Decision-Oriented Case Studies and the System Failure Case Studies focus on high-profile incidents with complex causes, Cases of Interest look at smaller incidents—even "close calls." These studies illustrate the importance of simple practices that can have serious consequences if improperly or inadequately executed. Cases of Interest turn to real-life stories to emphasize the value of best practices that might otherwise seem insignificant.

Decision-Oriented CASE STUDIES

OFFICE OF THE CHIEF KNOWLEDGE OFFICER, GODDARD SPACE FLIGHT CENTER

Decision-Oriented Case Studies walk participants through the story, pausing at crucial decision points to ask the participants how they would have responded to the situation. These studies attempt to recreate the situation by giving participants only the information that was available to decision-makers at the time. The case study may have an ambiguous conclusion; emphasis is not on what the right decision would have been but rather on the decision-making process.

At Goddard, we have found that the case-study method is especially effective in forums in which key players in the project are present. Whenever possible, case-based workshops at GSFC involve central personnel from a project, mission, or program, providing opportunities for key players to present material, reflect on project insights, and share contextual knowledge. By hearing directly from those who were intimately involved with the actual events, participants have the benefit of learning from the decision-making process itself.

How to use a Decision-Oriented Case Study

The decision-based cases included here are designed to provide you with enough context for an engaged discussion about the topic. They purposely do not give you all the information as most real life decisions are made with less than perfect information. Usually it takes at least an hour for each case study. The standard case hour is broken up as follows:

10 minutes	Read and familiarize yourself with the case
10 minutes	Discuss the case with other people at your table
15 minutes	Discuss the case as a large group with a facilitator
25 minutes	Interact with the expert, ask questions, seek lessons

Some case studies include a teaching note and epilogue. The epilogue finishes the story that the case study leaves deliberately open-ended; the teaching note demonstrates how to use the case to generate discussion and critical thinking in the classroom. The teaching note may also include specific technical details or fill intentional knowledge gaps in the case study.

These studies are meant to inspire thinking and conversation. They do not provide conclusive answers; they sharpen participants and equip them for the tasks lying ahead. Instead of learning a few principles, participants practice the decision-making skills that lead to success.

National Aeronautics and Space Administration

NASA Case Study GSFC-1009C-1

TDRSS: Fixed-Cost versus Cost-Plus Contracting

In the early days of the U.S. space program, the system of controlling and collecting data from low Earth-orbiting satellites included a series of ground stations scattered around the world. This worked well because the satellite population and data rates were low and signal strength was high. However, passes were short, because of the low altitude of the spacecraft. Also, more spacecraft were coming online. More contact with the spacecraft required more ground stations. This was both a workforce problem and a political problem. Some countries were not interested in cooperating with the United States in hosting ground stations, and several critical NASA ground stations closed just before major space missions owing to political instability in host countries.

First-generation tracking and data relay satellite, artist's concept. NASA image

By the late 1960s, low Earth-orbiting satellites were in view of the existing ground stations only about 15% of the time. The proposed manned missions would require more continuous coverage, even if the existing ground network was augmented with the expensive space-tracking aircraft and ships used in the *Apollo* network. The

proposed solution was to substantially increase coverage with a series of specialized geosynchronous communications satellites tracking the low Earth-orbiting satellites and relaying the data to a single U.S. ground station. This concept, called the Tracking and Data Relay Satellite System (TDRSS), would provide continuous coverage and keep all ground-system assets on U.S. soil.

As early as 1967, within 10 years of the start of the U.S. space program, phase A and B definition studies for a possible geosynchronous satellite system were launched at the Goddard Space Flight Center (GSFC). Such a system would include at least two Tracking and Data Relay Satellites (TDRSs) in geosynchronous orbits that could track low Earth-orbiting satellites over most of their orbits and relay their data to a U.S.-based ground station that was constantly in view. From there, the data would be relayed to the appropriate science centers. The advantages would be significant: very long passes, high data rates over extended parts of the orbit, and more satellites accommodated. Perhaps most importantly, the number of ground stations in other countries could be reduced.

These studies continued into the early 1970s and included the successful demonstration in 1974 of the capability of the space-based tracking system. Thus, it was decided to go ahead with TDRSS. There was, however, a potential problem with funding the system.

Financing

In the mid-1970s, NASA was under severe budgetary pressure because of high inflation and the end of the *Apollo* program. The agency had to trim the budget to fund the shuttle program. TDRSS would be very expensive, involving a number of spacecraft and a sophisticated ground system, and NASA's administrator did not want to ask Congress for appropriations that might interfere with shuttle development.

A solution was proposed that instead of building its own new system, NASA could lease communication services from a commercial provider. The contractor would be asked to build the system with private financing and lease back services to NASA for at least 10 years. NASA would pay for those services over that period using appropriated funds. The system would also have commercial communications capabilities. The revenue from the NASA lease and the commercial income would pay for the system and provide the profit for the company. The expectation was that NASA could save money with such an arrangement.

When the private-financing plan fell through, it was decided that industry participants would borrow money directly from the Federal Finance Bank (FFB), part of the U.S. Treasury. The required special permission was obtained from the U.S. Congress, and NASA guaranteed the loan. The money would be "off-budget" for NASA initially and paid back with appropriated funds during the 10-year operation period. An interesting part of the arrangement was that it allowed the contractor to borrow money from the FFB without NASA's approval though the contractor was required to notify NASA in writing when it withdrew funds.

The TDRSS Program was established by NASA in 1973 and assigned to GSFC. Acquisition for the first series began in 1974 with the request for proposals (RFP), and in 1976 a 10-year, fixed-price (FP), leased-services contract worth $786 million was signed. The prime contract for the first series of six spacecraft and the ground system was won by Western Union's subsidiary Western Union Space

Communications (WUSC). TRW, Inc., was subcontracted for the space segment and Harris Corporation for the ground segment, both signing FP contracts for their respective deliverables.

As the government was buying what it thought was a known service over time, it chose to enter into an FP contract with WUSC for leased services in order to avoid large, up-front capital outlays that would compete with shuttle development. According to the government's Federal Acquisition Regulation (FAR) Web site, an FP contract "provides for a price that is not subject to any adjustment on the basis of the contractor's cost experience in performing the contract. This type of contract places upon the contractor the maximum risk and full responsibility for all costs and resulting profit or loss." The more typical (for NASA) cost-plus award fee (CPAF) contract is defined by FAR as,

> A cost-reimbursement contract that provides for a fee consisting of (a) a base amount (which may be zero) fixed at inception of the contract; and (b) an award amount, based upon a judgmental evaluation by the Government, sufficient to provide motivation for excellence in contract performance.

Since NASA was not directly involved in TDRSS development and would not own the assets, the FP arrangement seemed appropriate.

The First Series

The TDRSS project office at GSFC had responsibility for both the space and ground segments, with a deputy project manager assigned to each. The NASA challenge was to develop three major systems simultaneously—the user, ground, and space segments. NASA retained total responsibility for developing the user segment and portions of the ground segment, and contracted with WUSC to develop the remainder of the system, including the space segment and the part of the ground segment that controlled the TDRSS constellation and served as a terminus for all TDRSS communications channels.

GSFC gave out contracts for user-transponder design and development to several companies, and designed and constructed an operations facility and computer complexes for TDRSS schedule planning and user orbit determination at GSFC. The contract for the remainder of the TDRSS space and ground assets was awarded to WUSC, based on low bid. TRW was to perform end-to-end system architecture, system design and engineering, ground- and space-segment architecture, and to design and build the space segment. Harris Corporation was to build portions of the ground system including the antennas and ground-communications equipment. The original launch readiness date for the first spacecraft was set for 1978. WUSC would borrow money from the FFB twice per month to fund development, which was to be repaid, including interest, by NASA.

The proposal stipulated dual-use spacecraft, meeting all government TDRSS needs and carrying a C- and Ku-Band communications-payload capability for commercial use.[1] One difficulty NASA had with the RFP was being able to specify the system functionality it needed to satisfy its service requirements 13 years into the future.

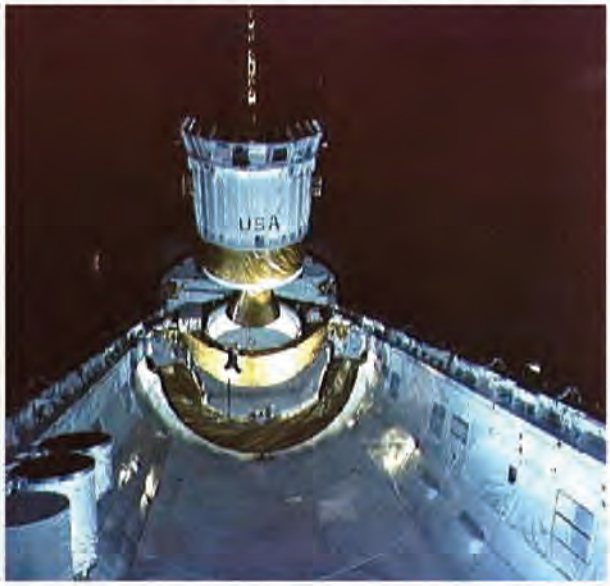
---

[1] The entire system was designated the Shared Services Tracking and Data Relay Satellite System (SSTDRSS). It consisted of the TDRSS program and the Western Union Advanced Westar Commercial Communication Program.

The WUSC plan was for two of the six satellites to be dedicated to TDRSS, one as an on-orbit spare available for rapid TDRSS or WUSC Advanced Westar (AW) replacement, and two of the remaining three to be dedicated to AW. The sixth was to be an on-the-ground spare to be used in the event of a launch failure and a replacement for the in-orbit spare if necessary.

Early Changes during Development

Early on there were problems and changes that had major effects on cost and schedule. These changes were government-driven and, under the FP arrangement, were not absorbed by the contractor. The first was a potentially severe radio-frequency interference problem caused by high-powered, ground-based radar transmissions over Eastern Europe. NASA was unaware of this problem when the RFP was written, so the system specifications did not take those into account. This could have changed the entire design, but the issue was resolved with no significant design changes.



TDRS-A deployed by Challenger STS-6, April 1983. NASA image

The real problem was the contract. With a CPAF contract, a GSFC team easily could have met with the TRW team and determined a solution together. A change order could have been issued quickly and the delay minimized. However, GSFC had bought off on the initial design and, under FP terms, the GSFC project team was not prepared to interact directly with TRW at first—it was to be "hands off." WUSC had no particular expertise in this matter; TRW did, but was not part of the GSFC–WUSC contract interface, so TRW waited for direction. WUSC wanted NASA–TRW interfaces to go through WUSC. One estimate put the cost of the delays at $70 million.

Other changes affecting cost and schedule included the decision to move TDRS-A from an expendable launch vehicle (ELV) to the shuttle for launch.[2] This was costly for two reasons. First, TDRS-A had to be changed to conform to shuttle safety standards, which consumed a lot of time working with Johnson Space Center (JSC) and Kennedy Space Center (KSC). Second, an Air Force inertial upper stage (IUS) had to be added to enable the spacecraft to get to synchronous orbit after being deployed by the shuttle in a low-Earth orbit. Headquarters held JSC responsible for the IUS-to-shuttle interface, which worked well, but the shuttle was still being developed, which complicated the process. For example, JSC did not have the shuttle load information. Those changes added approximately $80 million.

---

[2] A potential weight problem was solved by going to the shuttle. When the propulsion system was sized in 1976, they forgot to include a weight budget for station-keeping fuel for the commercial function. (NASA did not require station keeping.) This could have added more than 1,000 pounds, which would have required a larger ELV—a Titan. That would have had to be absorbed by the contractor per this FP contract.

In 1980, while TDRS-A was in integration and the ground system was far along, the Air Force decided that it was necessary to upgrade the communications security between the ground station and the flight segment, so encryption was added to the link.[3] This required major changes to the hardware and software in the ground segment and to the hardware in the flight segment, costing an estimated $50 million to $100 million. More money was borrowed from the FFB.

The TDRS-A launch, originally scheduled for 1978, was eventually delayed to 1980 because of the earlier changes. The shuttle development and Air Force delays slipped launch to April 1983.

Space-Segment Development

Technical development went relatively well, but there were some difficulties. WUSC was the prime contractor but had little experience developing space systems. As a result, communications among contracting parties was often difficult, especially between GSFC and WUSC. Eventually the GSFC team was able to work with TRW despite WUSC, which was mostly concerned with maintaining the viability of the commercial C- and Ku-Band links and resisted any changes that might affect them. This was to be expected under an FP contract. WUSC had neither the financial strength nor the inclination to assume liability for correcting space- or ground-segment flaws. Consequently, there was a temptation to accept the service penalties that resulted from operational outages rather than making the fixes required. NASA found that unacceptable.

White Sands Ground Terminal. NASA image

Ground-Segment Development

The TDRSS ground segment consisted of multiple parts, some developed by GSFC through the WUSC contract and some developed within GSFC. The data from the user satellites (NASA and other government users) and from the commercial links would flow through the TDRSs to the ground station in White Sands, New Mexico. White Sands Ground Terminal (WSGT) was developed by WUSC. In the same building was the NASA Ground Terminal (NGT). All government data flowed from the WSGT to the NGT where it was quality-checked and sent to mission control centers and data-processing facilities. Some mission and status data were sent to the Network Control Center (NCC) at GSFC. The NCC, in

[3] In 1981, TDRSS was declared a national asset, meaning that it would fulfill critical national needs. This was driven by the Air Force and the shuttle's dependence on TDRSS to provide nearly continuous contact with the ground.

turn, returned schedule and state vector data back through the NGT to the WSGT for control of the space segment. The commercial data, captured by a separate C-Band antenna, flowed from the WSGT straight to other commercial facilities.

Contractually, the ground and space segments were similar. The difficult interface on the space segment with WUSC between GSFC and TRW was duplicated in the ground segment. WUSC was between GSFC and Harris and between Harris and TRW. A more-logical arrangement would have Harris as a subcontractor to TRW. Despite the clumsy arrangement, GSFC, TRW, and Harris fixed the problems, but the initial lack of functional requirements in the TDRSS service specification did have an impact. As the real requirements were brought to light, most flowed directly into the ground-segment specification. A relatively simple 100-page ground-segment specification grew to more than 300 pages.

Developing the WSGT software proved to be far more difficult than building the hardware. Changes and problems were numerous, including quality problems, adding encryption, and other requirements' changes. The WSGT was built by WUSC to commercial standards—not up to NASA standards. Multiple-access (MA) service did not work well at first and developed a bad reputation in the user community, which put larger-than-expected demands on the single-access service. Unstable MA ground receivers were the primary issue.

First-Series Launch Record

- **TDRS-A** launched April 5, 1983
- **TDRS-B** destroyed January 28, 1986, in the *Challenger* disaster
- **TDRS-C** launched September 29, 1988
- **TDRS-D** launched March 13, 1989
- **TDRS-E** launched August 2, 1991
- **TDRS-F** launched January 13, 1993
- **TDRS-G** launched July 13, 1995 (replacement for TDRS-B)

Contractor Changes

Modification (mod) 37 to the contract, effective June 27, 1980, was a novation[4] of the contract to the Space Communication Company, known as Spacecom. Western Union sold 25% of the shares to Fairchild and 25% to Contel Federal Systems, retaining 50%. This event is known as "reformation." Between 1984 and 1986, Contel bought all of Spacecom, and by mod 555 on February 15, 1989, the contractor was Contel Federal Systems. The GSFC project had been frustrated with Western Union, because of its lack of expertise in the space field, and in fact Western Union had been seen as an

[4] Novation is the substitution of one-performance obligation with a new obligation, or replacing a party to an agreement with a new party.

impediment between TRW/Harris and GSFC. Now there was a sense that the new partners brought at least some technical expertise to the table, so the situation improved somewhat.

During 1989 to 1990, a "mini-reformation" took place. At that time, there were three spacecraft in orbit. Previously, NASA owned nothing and had bought services from WUSC/Spacecom. Contel now had TRW and Harris as subcontractors. The service contract had small penalties for interruptions of service, but the FFB loan had to be repaid whether the users were served or not. On the other hand, the daily TDRSS operating costs had to be paid out of the revenue stream from the Advance Westar (AW) C- and Ku-Band services. Consequently, Contel had a heavy incentive to convert TDRSS assets to AW assets in the event of an AW failure, but almost no incentive to convert an AW asset to TDRSS in the event of a TDRS failure. It became obvious to the government that something had to be done about the contractual arrangement.

You Decide

- *Sketch a diagram of the organizational structure of the TDRSS program, showing the relationships between the key organizations. What implications does this kind of structure have for project management and performance? Do you see any parallels with your projects?*
- *What would you recommend regarding the current TDRSS contractual arrangement? Should you stay the course? Renegotiate the terms? How about buying out the contractor?*
- *What might be some of the unanticipated consequences of contracting relationships?*
- *How can the lessons learned from TDRSS apply to future NASA projects?*

National Aeronautics and Space Administration

NASA Case Study Epilogue GSFC-1009E-1

TDRSS: Fixed-Price versus Cost-Plus Contracting

By 1990, the government concluded it had little choice but to buy the entire system outright. At the mini-reformation, the contract was converted from a service contract to a hardware contract and NASA took ownership of the spacecraft. Modification (mod) 1 of the new contract, signed July 1, 1990, assigned the TRW, Inc., spacecraft contract to NASA.

In the eyes of both the GSFC project and TRW, this was a major improvement. Contel, however, still owned the ground system, White Sands Ground Terminal (WSGT) in New Mexico, the operation of which NASA found unsatisfactory because NASA was unable to readily implement needed changes and operate the system in an optimum manner for NASA needs. Thus, the government wanted control of the ground station. To get title to the ground station before the end of the 10-year service period, the government's *quid pro quo* was to give Contel additional years of ground-system operations and maintenance. As part of the mini-reformation, the government now owned the ground system, and Contel supplied operations and maintenance.

Additionally, the government bought the commercial C-Band capability from Contel as it took ownership of the spacecraft. The C-Band capability, however, remained on the spacecraft through TDRS-F. This capability was later leased to another company and is still in use today on TDRSs-D, -E, and -F.

After the *Challenger* was lost in January 1986 with the second TDRS spacecraft aboard, the U.S. Congress funded a replacement program for the spacecraft. The replacement would be designated TDRS-G and launched on July 13, 1995. This was prior to the mini-reformation, so Spacecom still held the fixed-price (FP) contract for the first six spacecraft still in development.

NASA decided to go ahead with a separate cost-plus award fee (CPAF) contract for TDRS-G, instead of adding it to the ongoing first series. It was a sole-source contract directly with TRW, most likely a

reaction to the difficulties encountered with the original fixed-price contract first with Western Union and then Spacecom. With the Spacecom contract was still in place, TRW was now working under two separate contracts, one an FP with Spacecom and a CPAF directly with GSFC.

In April 1992, the new administrator took the position that the agency was overcommitted to large, expensive programs. He suggested that it was necessary only to replicate a TDRS-G spacecraft, without the proposed changes. In addition, because the first series was lasting beyond expectations, it was difficult to justify a large new fleet. After a series of reviews in 1992, the program was redirected to a much more modest follow-on program known as the Replenishment Program. By that time, the number of spacecraft was down to three.

The GSFC director's position was that it should be a CPAF contract and that NASA should purchase the launch vehicle. NASA had developed very thoroughly detailed specifications and had worked hard to develop adequate competition within the industry. GSFC believed that sufficient experience was gained on TDRS-A through TDRS-G and that the changes were not that extensive, so FP made sense for the government. A $486 million FP contract was awarded to Hughes (later bought by Boeing) in February 1995 for TDRSs-H, -I, and -J. TDRS-H was launched on June 30, 2000; TDRS-I on March 8, 2002; and TDRS-J on December 4, 2002. The latter were delayed by GSFC, because the previous generation lasted longer than expected. In 2007, Robert Spearing, NASA deputy associate administrator for space communications, put the collective cost for TDRSs-H, -I, and -J at about $800 million to build and launch.

Initially, NASA refused to accept TDRS-H from Boeing because it was launched with a faulty phased array antenna. As a result, signal strength was not improved over the first TDRSs as promised, and Boeing agreed to refund NASA $35 million. Shortly after launch on March 8, 2002, TDRS-I was discovered to have a blocked valve resulting in two onboard propellant tanks that could not be pressurized to feed the craft's maneuvering engine. This meant that the craft would not be able to boost itself into geostationary orbit, essentially becoming space debris. In what Boeing called "a remote-control coronary bypass," controllers rerouted fuel tank pressurant around the blockage and conducted a series of engine burns over four months. On October 1, 2002, the last burn put the craft into its storage orbit at 22,300 miles above Earth.

Artist's conception of basic TDRS design for H through L. NASA image

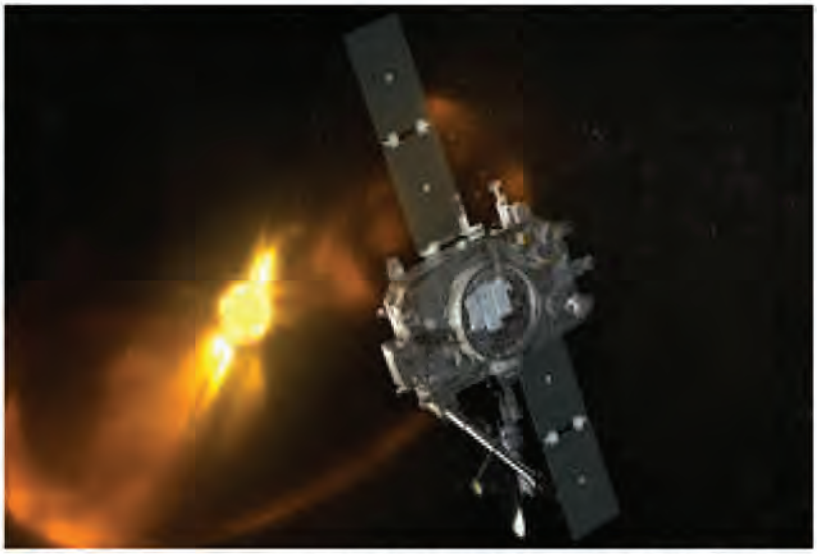
In late December 2007, NASA selected Boeing to build the next generation of TDRSs. A $695 million contract—or $1.2 billion, if all options are exercised—was signed for design and manufacturing of two spacecraft and upgrades to NASA's TDRSS ground terminals. TDRS-K is scheduled for launch in 2012 and TDRS-L in 2013. The options are for two additional satellites—TDRS-M and TDRS–N—to be launched in 2015 and 2016, respectively.

National Aeronautics and Space Administration

NASA Case Study GSFC-1017C-1

STEREO: Organizational Cultures in Conflict

NASA's Solar Terrestrial Probes (STP) Program, created by the Office of Space Science, offered a continuous sequence of flexible, cost-capped missions to investigate the Earth–Sun system. STP missions used a blend of *in situ* and remote-sensing observations, often from multiple platforms, to study the Sun and Earth as an integrated system.

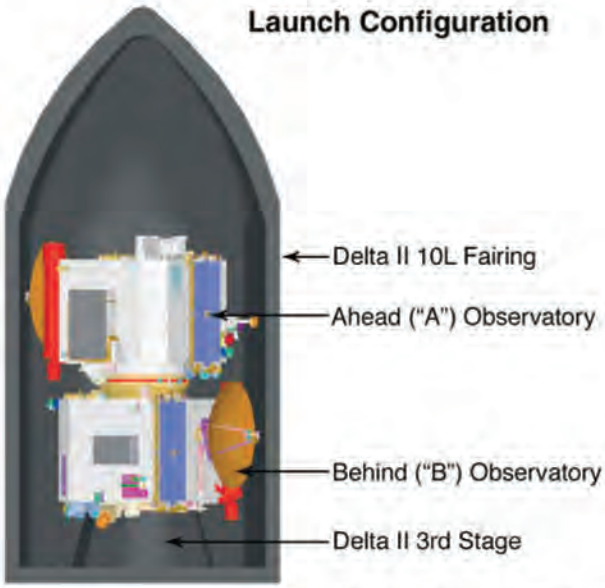


The loop of a coronal mass ejection heads straight toward a STEREO satellite in this artist's conception. NASA image

The *STEREO* (Solar Terrestrial Relations Observatory) mission was conceived to advance three main program objectives: (1) understand the changing flow of energy and matter throughout the Sun, heliosphere, and planetary environments; (2) explore the fundamental physical processes of space plasma systems; and (3) define the origins and effects of variability in the Earth–Sun connection.

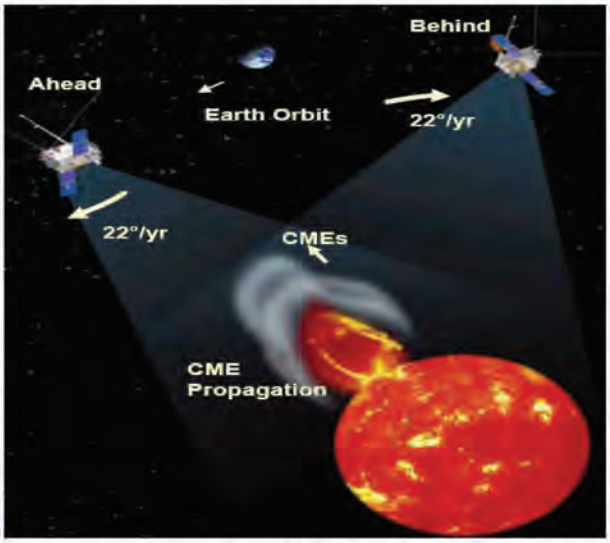
The *STEREO* Mission

Goddard Space Flight Center (GSFC) began the *STEREO* mission in July 1999. *STEREO* was designed to offer a new perspective on solar eruptions by imaging coronal mass ejections (CME) and background events from two nearly identical observatories simultaneously. To obtain unique views of the Sun, the twin observatories would have to be placed into rather challenging orbits where they would be offset from one another. One observatory would be placed ahead of Earth (*STEREO* A) in its orbit and the other behind (*STEREO* B). Just as the slight offset between one's eyes provides depth perception, this placement would allow the *STEREO* observatories to acquire 3-D images of the Sun. A series of lunar swing-bys would be used to place the observatories in their orbits.



Launch configuration of the observatories inside the Delta II rocket. NASA image

STEREO was the third mission in NASA's STP program and was scheduled to launch in February 2006 on board a single *Delta II* launch vehicle.



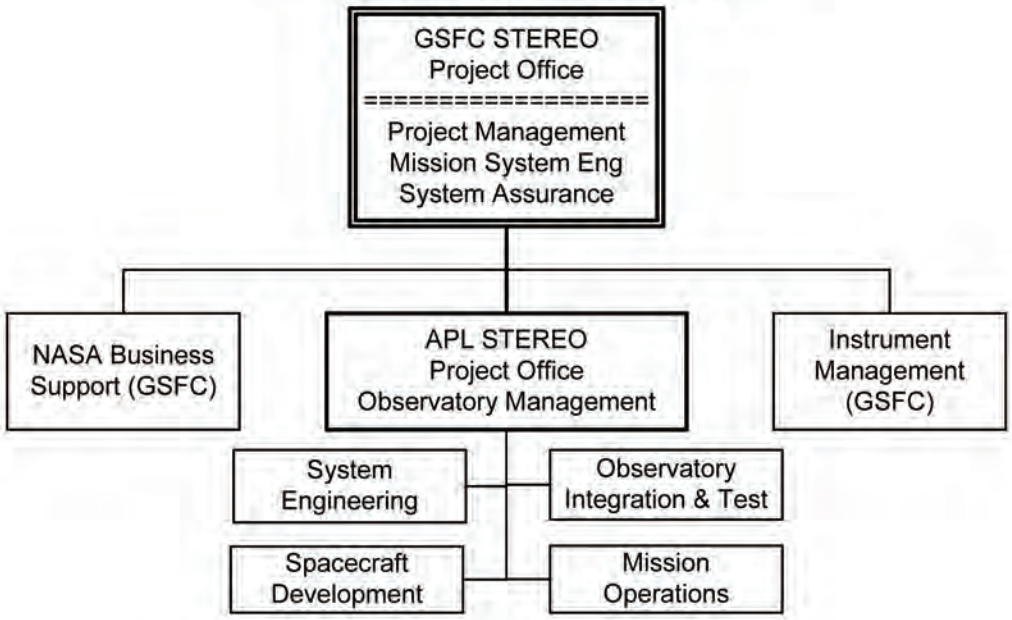
Artist's representation of STEREO observatories, one ahead of Earth's orbit and one behind, which will trace the flow of energy and matter from Sun to Earth and reveal the 3-D structure of coronal mass ejections. NASA image

Each of the twin *STEREO* observatories would carry two instruments (PLASTIC and SWAVES) and two instrument suites (SECCHI and IMPACT). This combination provided 16 instruments per observatory, including coronagraphs, imagers, burst trackers, plasma sensors, and magnetometers. The total cost for the two-year mission would be approximately $400 million for the spacecraft, instruments, launch vehicle, ground and mission operations, and data analysis.

Project Organization

Goddard's STP program office was managing the mission, instruments, and the mission's science center. The Applied Physics Laboratory (APL) at Johns Hopkins University was responsible for designing, building, and operating the twin observatories for NASA. The instruments were being developed and provided by collaborations of university and international partners. APL also designed, built, and currently operates the first STP spacecraft, *TIMED* (Thermosphere Ionosphere Mesosphere Energetics and Dynamics), which launched on December 7, 2001.

STEREO Organizational Chart



Dealing with Culture

APL's space department culture and values were rooted in the early history of the American space program. APL spacecraft history began in 1959 and counted more than 60 successful missions at the time of the *STEREO* mission. Many of those involved development and fielding of the first satellite navigation constellation for the U.S. Navy. Later APL developed spacecraft and space instrumentation for a variety of military missions. For those projects, APL had worked autonomously, with very limited oversight from the sponsors. It thus developed a culture that valued independence, technical performance, and short development schedules (typically three years). APL had also handled a number of NASA-sponsored missions, including *AMPTE* (Active Magnetospheric Particle Tracer Explorers), *ACE* (Advanced Competition Explorer), *NEAR* (Near-Earth Asteroid Rendezvous), and *TIMED*.

The individual centers and partners comprising NASA missions typically brought different management models to a program or project and this was no different for APL working on *STEREO*. At first the cultural differences seemed easily surmountable, but a survey of the project team revealed that the issues were more deeply rooted and worthy of management's attention. Comments (see next page) indicated how culture could hinder or prevent success. Recognizing that there were cultural issues between Goddard and APL personnel, both teams decided to hold several offsite retreats, including one in May 2004. The core outcome of this retreat was the establishment of an operating agreement (see next page) to help the APL and Goddard teams interact as effectively as possible.

Feedback from the Team Survey[1]

GSFC's Comments

- "APL seems to place more emphasis on cost and schedule, rather than performance. In more than one instance, they have identified concerns regarding a NASA-proposed implementation, where had they applied the same criteria to their approach, the APL solution would have been found to be inferior. They appear to be willing to accept more risk—basically a 'commercial' mind-set."
- "I think that APL's vision is somewhat limited to APL only."
- "APL has their own focus again; I don't think it's by any means the same as NASA/GSFC."
- "APL needs to accept GSFC/NASA's involvement and move forward as a team. Every member has a place and a role on this mission."
- "Not blaming is VERY hard—almost across the board—in our dynamic with APL. We could use some guidance or coaching."

APL's Comments

- "Although we have had times where we appreciate each other's work, the general mood is one of mistrust."
- "Because trust has diminished on the project, we have become very guarded in what we say."
- "I believe both the Goddard and APL teams share equal values. I also believe that the values are noble. The breakdown seems only to be limited by what we perceive to be the best path toward achieving a common goal while living within these shared values."
- "The distractions of politics, petty disagreements, personal agendas, and unresolved conflicts by both APL and GSFC are destructive behaviors standing in the way of a common goal."
- "Both organizations have a long successful history, but the approaches to those successes have been different. Both organizations are comfortable with their approach. We too often get bogged down in wanting to maintain 'our' way."
- "APL has 'the APL way' and Goddard has 'the Goddard way'—each is new to the other."
- "Each organization is very locked into their paradigm of how to execute a program."

[1] These are actual comments excerpted from the survey and are representative of the type of comments received.

The Operating Agreement[2]

General Operating Agreements

The GSFC and APL *STEREO* Integration & Testing Teams have a "trusted contractor–customer" relationship

- We will operate with a badgeless culture—we are clear about the contractor–customer interface; anyone can accept direction from the appropriate lead.
- We will share credit for success and responsibility for failure.
- We will trust one another and will work to maintain that trust.
- We will operate with clear lines of responsibility.
- We will have clear ground rules and open access and communication within those boundaries.
- We will work issues at the lowest levels practicable.
- We will clearly define the I&T process.
- We will jointly define a "successful" test.
- We will jointly agree on priorities and work off one master schedule.
- GSFC will defend APL to NASA management.
- GSFC doesn't give "work direction"—we give information.
- GSFC will be at the table during testing—they have open access.
- We recognize and respect that both GSFC and APL add value.
- We are willing to learn from one another.

The Challenge

Having identified the cultural challenge and documented it with the survey, answer the following questions and justify your rationale:

- *How should you respond to the survey results?*
- *How can this feedback from the survey and the operating agreement help you ensure a successful launch and valuable science results?*
- *What would be your actions regarding the culture issues?*
- *What, if any, time and resources would you spend tackling this challenge?*

---

[2] These so-called "top-line principles" were agreed to at the May 2004 team retreat. There were also more supporting details not supplied here for sake of brevity in the case.

National Aeronautics and Space Administration

NASA Case Study Epilogue GSFC-1017E-1

STEREO: Organizational Cultures in Conflict

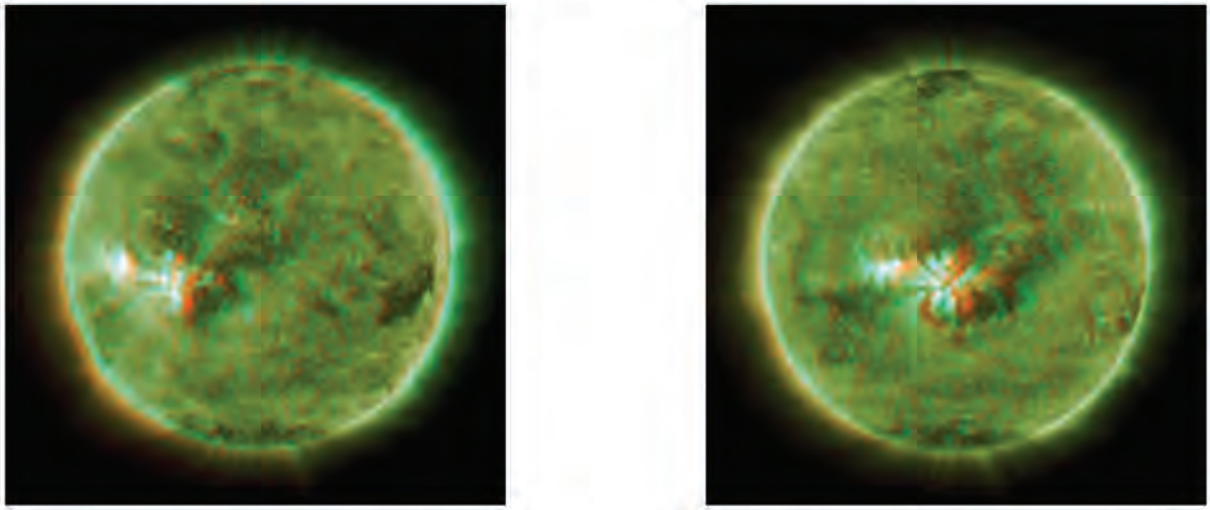
The STEREO A (Ahead) and B (Behind) observatories were successfully launched from Cape Canaveral, Florida, on October 26, 2006, at 8:52 p.m. for a mission of at least two years.

The original launch target of February 2006 slipped owing to a succession of problems, the most significant involving Boeing's second-stage oxidizer tanks for its *Delta II 7925* launchers. Boeing engineers discovered that a tank at their Decatur, Alabama, plant identical to that being used for the STEREO launch was leaking as a result of metal thinness. All such tanks had to be checked, which meant the STEREO launcher was destacked and the tank checked from the inside. Verification, restacking, and refilling resulted in a three-month delay. Other delays included an earlier hydrazine propellant leak, instrument development difficulties, battery issues, and the usual launch-window considerations.

STEREO liftoff from Cape Canaveral Air Force Station, October 26, 2006. NASA image

On October 26, launch day, the *Delta II* lifted the two craft into highly elliptical geocentric orbits, their apogees reaching the Moon's orbit. On December 15, 2006, during the fifth orbit, the pair swung by the Moon for a gravitational swingby maneuver. At that point, STEREO A ejected to a heliocentric orbit inside Earth's orbit, while STEREO B remained temporarily on a high Earth orbit. STEREO B encountered the Moon again on January 21, 2007, ejecting it from Earth's orbit in the opposite direction of STEREO A. STEREO B entered a heliocentric orbit outside Earth's orbit, with the result that A and B completed their respective sun orbits in 347 and 387 days respectively. With STEREO A moving faster and going closer to the Sun, the two craft together produce stereoscopic, 3-D pairs of images.

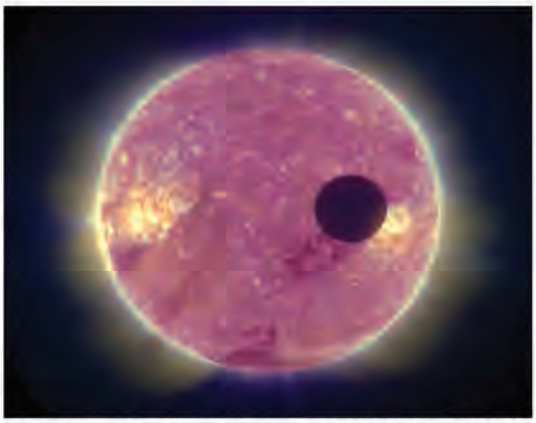
At a news conference on April 23, 2007, NASA unveiled 3-D anaglyph video and images of the Sun that had been acquired by the STEREO craft.



By combining images taken almost simultaneously from the A and B spacecraft, researchers have generated a 3-D sequence of images that track an active solar region over about a one-week period. The images were all taken in the 171 Angstrom wavelength of extreme ultraviolet (UV) light. Active regions, which are areas of intense magnetic activity, appear brighter in UV light. The region is seen moving from left to right as the Sun's rotation carries it along. Arcing loops above the active region reveal million-degree Celsius particles spinning along magnetic field lines. These images can be viewed with red and cyan 3-D glasses. NASA image

On February 25, 2007, there was an eclipse of the Moon when it crossed the face of the Sun, but it could not be seen from Earth. It could be seen, however, from the STEREO B spacecraft in its orbit around the sun, but trailing behind the Earth. STEREO B is approximately one million miles from the Earth, 4.4 times farther away from the Moon than we are on Earth. As a result, the Moon will appear 4.4 times smaller than what we are used to (but much larger than, for example, the planet Venus appeared when it transited the Sun as seen from Earth in 2004.) This alignment of STEREO B and the Moon was not just due to luck. It was arranged with a small tweak to STEREO B's orbit the previous December. This is quite useful to STEREO scientists for measuring the focus and the amount of scattered light in the STEREO imagers and for determining the pointing of the STEREO coronagraphs. The sun as it appears in the images and each frame of the movie is a composite of nearly simultaneous images in four different wavelengths of extreme ultraviolet light that were separated into color channels and then recombined with some level of transparency for each. To put STEREO's success into perspective, Dr. Michael Kaiser,

STEREO project scientist from Goddard Space Flight Center (GSFC), said: "The improvement with STEREO's 3-D view is like going from a regular x-ray to a 3-D CAT scan in the medical field."



Eclipse of the Moon as seen by STEREO B. NASA image

The instruments' more accurate images are anticipated to have great scientific possibilities. "With STEREO's 3-D imagery, we'll be able to discern where matter and energy flows in the solar atmosphere much more precisely than with the 2-D views available before. This will really help us understand the complex physics going on," said Dr. Russell Howard of the Naval Research Laboratory, principal investigator for the SECCHI suite of telescopes on the spacecraft. The images are more precise and they shed light on what scientists could only model before. Dr. Madhulika Guhathakurta, STEREO program scientist at NASA HQ, said that the STEREO craft are able to image solar disturbances "the entire way from the Sun to the Earth. Currently, scientists are only able to model this region in the dark, from only one picture of solar disturbance leaving the Sun and reaching only a fraction of the Sun–Earth distance."

The STEREO observatories have performed to expectations and are being fine-tuned throughout the mission for imagery of even greater scientific impact. Before it could get that far, though, the project management team had to overcome some partnership issues. According to Mark Jarosz, STEREO observatory manager, "After the first review, Nick [Chrissotimos, project manager] said, 'No, we're a Goddard project, we're managing it.' A light switch went off, and changed the mindset." This attitude might have come from differing attitudes from senior management at both GSFC and NASA HQ: One wanted GSFC to take a hands-off approach, the other wanted GSFC to take a more active oversight role. "In the end," Chrissotimos said, "GSFC had to play a more active management role." The important management lesson for Chrissotimos was that a project "should not come down to 'you're a contractor' or 'you're a partner.' It should be what's best for the project."

Ed Reynolds, the STEREO project manager for Applied Physic Laboratory (APL), offers a similar perspective:

> Before we got there [to a point of open communication], communication was being controlled through a bottleneck at APL—to control the project. We worked really hard to get that communication open, and trust started to be established. One of the ways [we opened communication] was that there were times when we needed a skill set and we went to Goddard and said, "Can you provide it?" We were trying to launch New Horizons at the same time and we were really stretched. It wasn't like they were writing negative reports about our skills. That really helped establish the trust.

The coinciding attitudes of the GSFC and APL project managers allowed the team to work together effectively and build a relationship of trust and communication. In summary, the GFSC–APL team found a way to break its cultural paradigm lock. Open, frank discussion at the team's offsite meeting led to the agreed-upon "top-line principles" that broke the impasse and led to stunning mission success.

National Aeronautics and Space Administration

Teaching Note for NASA Case Study GSFC-1017T-1

STEREO: Organizational Cultures in Conflict

Synopsis

STEREO was the third project in NASA's Solar Terrestrial Probes (STP) Program for studying the Sun–Earth system. Initiated in 1999, STEREO (Solar-Terrestrial Relations Observatory) was slated as a two-year mission scheduled for launch in early 2006. It was designed to provide unique, three-dimensional views of the Sun using two nearly identical space-based observatories in offset orbits, one ahead (STEREO A) of Earth in its orbit, the other behind (STEREO B). Operating simultaneously, they would be able to image events in 3-D.

The project was a collaboration between Goddard and Johns Hopkins University's Applied Physics Laboratory (APL), two organizations with long histories in spaceflight projects but dramatically different organizational cultures. The differences became increasingly evident during the early stages of the project. Eventually friction, mistrust, and confusion over roles and responsibilities threatened to derail the project. Managers, facing political pressure to succeed for the future of the STP program, took creative steps to bridge the gap between a traditionally process-oriented organization (Goddard) and a people-oriented one (APL) and to get the mission back on track.

Purpose

The case of STEREO is a story of an ambitious and programmatically important space-science project running up against daunting organizational culture issues. The learning objectives center primarily on how to deal with cultural differences as identified in a cross-organizational survey that revealed how "culture gets in the way of success."

Key learning points are:

- Performance, cost, and schedule may be weighted differently in disparate organizational cultures, leading to difficult-to-manage conflicts.
- Organizations can become "locked into paradigms" that seem irreconcilable.
- Excessive "ownership" and disagreement over management responsibilities can be potentially fatal to a project.
- Managing inter-organizational expectations and relationships is as vital a part of project management as resolving cultural differences and may be critical to mission success.

Discussion

After descriptions of the mission, the spacecraft, and the project organization, the case focuses on the relationship between GSFC and APL. The reader (or workshop participant) is asked to respond to the culture issues and to consider possible resources and actions to overcome "culture shock" (as the project manager would later describe it) and make a productive union out of "a shotgun marriage."

The comments from GSFC and APL team members, gathered through the survey, bring the case to life and are effective in stimulating thought and discussion. In addition, a copy of "top-line principles" from an operating agreement between the two organizations, forged during an offsite team retreat held to facilitate interaction, is enlightening. The operating agreement may be used as an epilogue or debrief following the discussion of ideas—to wit, here is how the team jointly decided to resolve its differences and move forward for the good of the project. Quotes from the NASA and APL project managers (below, respectively, and included in the epilogue) are instructive.

- Goddard PM: "In the end, GSFC had to play a more active management role." A project "should not come down to 'you're a contractor' or 'you're a partner.' It should be what's best for the project."
- APL PM: "Before we got there [to a point of open communication], communication was being controlled through a bottleneck at APL—to control the project. We worked really hard to get that communication open, and trust started to be established. One of the ways [we opened communication] was that there were times when we needed a skill set and we went to Goddard and said, 'Can you provide it?' We were trying to launch New Horizons [Pluto reconnaissance mission with Goddard] at the same time and we were really stretched. It wasn't like they were writing negative reports about our skills. That really helped establish the trust."

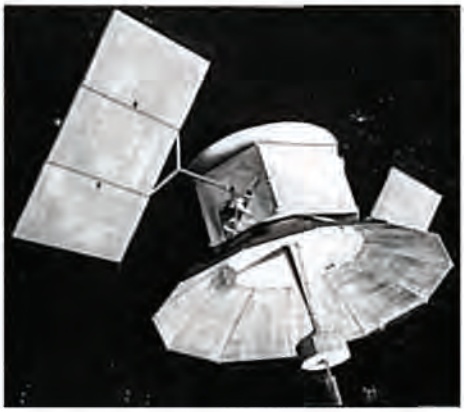
National Aeronautics and Space Administration

NASA Case Study GSFC-1008C-1

Atlas Centaur-67: Go or No Go for Launch?

Since 1968, NASA had flown dozens of scientific, defense, and commercial payloads into space on the *Atlas Centaur* rocket. On March 27, 1987, *Atlas Centaur Mission 67* (*AC-67*) sat on a launch pad at Cape Canaveral, Florida, waiting to carry the U.S. Department of Defense Fleet Satellite Communications (*FLTSATCOM*) F-6 spacecraft into orbit.

FLTSATCOM was a constellation of military satellites that served as a global ultra-high frequency (UHF) link among U.S. Navy aircraft, ships, submarines, and ground stations. A high-capacity space-borne communications system, it provided shore-to-fleet and single-way communications. It was also used for high-priority communications with the U.S. Air Force Strategic Airlift Command aircraft, the E-3A airborne warning and control system, and the presidential command structure. Four operational satellites positioned around the globe in near-equatorial geosynchronous orbits, as well as a fifth, on-station spare spacecraft, made up the *FLTSATCOM* system.



FLTSATCOM satellite in orbit. NASA image

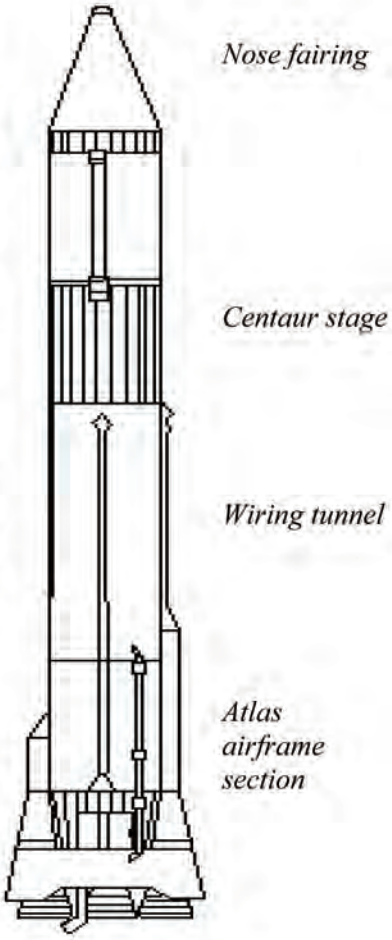
The *Atlas Centaur* was an expendable launch vehicle (ELV) used by NASA to place the *FLTSATCOM* spacecraft into geostationary transfer orbit (GTO). An apogee kick motor was employed to achieve the final mission orbit.

Launch Day: Black Clouds

On the scheduled launch day for *AC-67*, the weather did not look promising. Thunderstorms were building throughout central Florida near the launch site. The launch team included weather officers and safety officers responsible for ensuring that all launch weather and safety criteria were met. The launch director, launch team members, management advisors, and spectators were gathered in the Mission Directors' Center (MDC). In the team environment, amidst the flurry of launch-preparation activity, it was not entirely clear who was an authority and who was an advisor. In addition, some of the two-way radios were not providing clear communications between the blockhouse and Kennedy Space Center. Messages had to be repeated for clarity, further adding to the confusion in the launch center.

As launch countdown proceeded, a squall line developed, producing thunderstorms in areas adjacent to the launch facility. The clouds and the deteriorating weather conditions were apparent to the launch team at the site. The launch criteria stated: "The flight path of the vehicle should not be through middle-level cloud layers 6,000 feet or greater in depth, when the freezing level is in the clouds."

A debate ensued in the launch center over the meaning of the weather criteria, with some questioning the reason for the cloud criteria. It did not look like a serious hazard, particularly in the context of NASA's *AC* track record: The agency had successfully launched 66 *Atlas Centaur* rockets in a row. Many members of the launch team felt that there was ample experience in the room to make the call. And on the Air Force side, the payload team was eager to use an available launch window for its $83 million spacecraft.



Typical Atlas Centaur configuration. NASA image

At the same time, a sidebar discussion of the weather criteria centered on vehicle icing concerns. One member of the team contacted a nearby U.S. Federal Aviation Administration (FAA) control center to gain insight from any aviation activity in the cloud cover. The FAA reported two recent flights through the clouds with no icing incidents noted.

This information was reassuring to the launch team members preoccupied by icing concerns—icing appeared not to be a risk. And the presence of clouds was not, in itself, a reason to halt the countdown. The team agreed to call the weather office for a final weather "go," just before launch.

Make the Call: Go... or No Go?

You are a member of the launch team in the MDC. There are 10 minutes to liftoff. You see the darkening cloud banks. You've heard the FAA's "no icing incidents" report, yet you still are not sure whether the launch weather criteria are being fully met.

At T–3 minutes, the weather officer gives a "go-for-weather"—which surprises some members of the team who are looking out the window at the black clouds. The launch director looks around the room for any other concerns…. T–2:55, :54, :53…!

What concerns, if any, would you voice to the launch director at this point, and what suggestions would you make?

Would you recommend launching? What is the rationale for your decision?

National Aeronautics and Space Administration

NASA Case Study GSFC-1006C-1

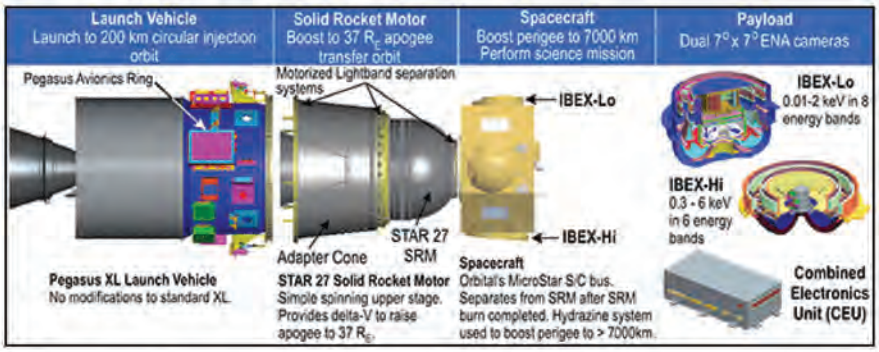
IBEX: Managing Logistical Exigencies

The Sun and solar system move through a part of the galaxy referred to as the "local interstellar medium," which is accumulated from material released by the stars of our galaxy by means of stellar winds, novae, and supernovae. *Interstellar Boundary Explorer* (*IBEX*) images will reveal global properties of the interstellar boundaries that separate our heliosphere from the local interstellar medium.

Early on in the *IBEX* satellite's development, it was decided that upon completion the spacecraft would be moved from the contractor's facility to the launch pad attached to the *Pegasus* launch vehicle rather than separately, as originally planned. The time has come for the move, and it is now obvious that the satellite-rocket assembly will not fit into the satellite-moving container for the 15-mile trip by truck.

Given the situation, the recommendation was to double-bag the stack in plastic for the move. However, this procedure is recommended only for much shorter trips. Time grows short as you and the team consider the technical, environmental, cost, schedule, and other risks.

What do you do?



Cross-section of Pegasus rocket with IBEX payload. NASA image

System Failure CASE STUDIES

NASA SAFETY CENTER

System Failure Case Studies (SFCS) examine complex and tightly coupled system failures. These studies aim to help readers apply mishap investigation findings locally and develop an enhanced awareness of how such failures occur. In a typical case study, an incident (usually technical) triggers a flurry of events that result in system-wide failure. The study discusses both the trigger event or "Proximate Cause" and the circumstances and climate surrounding the event, the "Underlying Issues." Because the Underlying Issues tend to focus on challenges in project management rather than technical problems specific to the incident, readers find useful applications in studies of events in a variety of fields.

System Failure Case Studies feature NASA mishaps as well as incidents from industry and other government organizations. They provide background information, illustrate the chain of events, analyze the Proximate Cause and Underlying Issues in the case, and summarize the outcome of the incident. They also discuss the case's applicability to NASA. The information they contain—including any conclusions about the incident—is substantiated by publically available reports. While engineers reading them may not be familiar with every case, they should be able to relate to the general scenario. Participants come away with a better understanding of how small elements in a system interact to create a volatile, unstable environment.

HOW TO USE A

System Failure Case Study

A System Failure Case Study can be read by an individual or in a small group. Each SFCS includes discussion questions to help participants draw conclusions, identify lessons, and apply the case to their work.

The NASA Safety Center hosts several types of facilitated sessions based on System Failure Case Studies. These include:

- Familiarization Brief (30 minutes): lecture-style presentation to a large group introducing the SFCS
- Issue Brief (30 minutes): lecture-style presentation to a large group using several related SFCSs to discuss a specific topic or concern
- Point-Counterpoint Workshop (1-1½ hours): small group workshop that breaks into teams to analyze the SFCS from two perspectives:
  - How this event could happen in this program
  - Why this event would not happen in this program

  Groups reconvene to present both perspectives
- Knowledge Café (4 hours, 5 case studies): small group workshop that breaks into teams to discuss a series of SFCSs
- Decision Making Seminar (1 SFCS, 4 hours): small group workshop that presents the scenario and breaks into teams to work through three phases of decision-making:
  - Determine risks
  - Prioritize top 3 risks
  - Establish risk mitigation plan

  Groups then reconvene to learn how the event played out and discuss applicability to their current program.

Visit http://nsc.nasa.gov (NASA only) or http://pbma.nasa.gov to read this month's SFCS or subscribe to the monthly publication. For more information about facilitated sessions, email nasa-nsc@nasa.gov.

National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

FEBRUARY 2008 VOLUME 2 ISSUE 2

Fire in the Cockpit

A seminal event in the history of human spaceflight occurred on the evening of January 27th, 1967, at Kennedy Space Center (KSC) when a fire ignited inside the Apollo 204 spacecraft during ground test activities. The 100% oxygen atmosphere, flammable materials and a suspected electrical short created a fire which quickly became an inferno. Virgil Grissom, Edward White II, and Roger Chaffee (the prime crewmembers for Apollo mission AS-204 – later designated Apollo 1) perished in the flames before the hatch could be opened .

BACKGROUND: THE SPACE RACE

In October of 1957, at the height of the Cold War, the Soviet Union launched the Sputnik satellite providing a global display of Soviet technological prowess and sending shock waves throughout the "free world." This marked the very public beginning of the "space race." Over the next four years the USA and the Soviet Union space programs evolved, learning from failures and celebrating successes. Then, in 1961, newly elected President John F. Kennedy declared that the USA would land on the moon and safely return by the end of the decade – thus initiating the Apollo Program and the race to the moon.

Mercury/Gemini Success – Overcoming Design & Quality Control Issues

Project Mercury was the United States' first human space flight program and accomplished six missions safely between May of 1961 and May of 1963 with a one astronaut crew. Historical records indicated that the Mercury Project struggled with design and quality issues associated with spare parts, batteries, improper soldering, improper installation of valves, and dirty regulators. Mercury was followed by the Gemini Project (two astronaut crew), which accomplished ten missions safely between March of 1965 and November of 1966. Notable design and quality issues included an electrical short on Gemini VIII in the control circuitry that caused early termination of the mission and a landing in a secondary recovery area. The Apollo Program accomplished the first manned missions in 1968 after seven years of component design, development and testing.

Figure 1: Grissom, White and Chaffee.

Apollo Spacecraft 204

AS-204 was built by North American Aviation (NAA) and shipped to KSC in August, 1966, despite the fact that there was still open work. That work and other engineering changes would be completed at KSC. The Command Mod-

A Tragic Fire Took the Lives of Three Astronauts Aboard Apollo 1.

Proximate Cause:

- A spark caused by an electrical short in a 100% oxygen atmosphere set fire to an abundance of flammable material

Underlying Issues:

- Vulnerable design and material choices for wiring, atmosphere, cabin materials, and hatch door
- Poor quality control and workmanship
- Inadequate provisions for emergency response
- Budget and schedule pressures resulted in the over-prioritization of speed

ule (CM) was received at KSC on August 26th and mated to the service module in September. More tests, reviews, and engineering changes ensued until January 6th, when the CM was removed from the test facility and mated with the launch vehicle on Pad 34.

Single vs. Two Gas Design

Competing design concepts included tradeoffs between the single gas (oxygen) versus two gas (nitrogen and oxygen) options, including: mass (500 pound weight penalty for tanks, tubing, and instrumentation for the two gas option); complexity and reliability (fewer failure modes with single gas design); vulnerability to the "bends" (nitrogen bubbles that could form in the body's tissues in the event of a micrometeoroid impact / decompression event); physiological problems associated with a 100% oxygen atmosphere (eye irritation, hearing effects, clogged chest); and increased fire hazard in a 100% oxygen atmosphere (to be mitigated through careful restriction of flammable materials). NASA had used the single gas design on Mercury and Gemini missions (over 1,000 hours of flight time) and on thousands of ground tests without a fire incident. The single gas option seemed a reasonable choice at the time.

Hatch Design

The CM was known as a "Block 1" design. One significant change from previous spacecraft designs was the hatch. Earlier hatches had opened outward, but the experience with premature release of a hatch on the Mercury MR-4 mission led to a redesign. The new hatch system was comprised of three sections, which required the removal of six bolts and opened inward. It was estimated that it took about 90 seconds to remove and stow the hatch and egress the crew.

What Happened?

The Fire

On January 27th, 1967, the Apollo 1 crew entered the spacecraft to perform an important launch countdown rehearsal test. The test commenced at 2:42 pm with hatch installation and subsequent oxygen cabin purge. For the next three hours, the crew and ground personnel performed tests. The countdown checklist continued to the point planned at 6:20 pm (T-10 minutes) when ground personnel would "pull the plugs" and the spacecraft would go into a simulated fuel cell environment. Awaiting clearance for this event, another hold was called. From 6:20 to 6:30 pm, there was routine troubleshooting of communications problems, and no events occurred that appeared to be related to the subsequent failure.

Tragedy struck at 6:30 pm, about 5 ½ hours after the start of the simulated countdown, when a significant transient in the AC Bus 2 voltage was observed. The transient indicated a major short circuit somewhere in the CM wiring. At 6:31:04.7, a crew member, speculated to have been Grissom, exclaimed "Fire! We've got a fire in the Cockpit!" At 6:31:16.8, another voice, thought to have been Chaffee, whose job it was to maintain communications in an emergency, said "We've got a bad fire – let's get out. We're burning up!" Before he could finish his sentence, the pressure inside the spacecraft had built up to more than two atmospheres. The spacecraft ruptured, and the cabin filled with toxic fumes. By 6:31:22, all voice and data transmissions had stopped.

Rescue efforts were hampered by the fire and smoke. Visibility in the environmentally controlled close-out room was essentially nonexistent. In all, 27 men were treated for smoke inhalation in fighting the fire. Efforts to remove the three-part hatch system began about one minute after the report of the fire, and the hatches were all removed by about 6:36 pm. By then, it was too late.

Proximate Cause

The report of the Review Board stated that "the fire was most probably brought about by some minor malfunction or failure in equipment or wire insulation… This failure, which most likely will never be positively identified, initiated a sequence of events that culminated in the conflagration." The most likely scenario, identified in the exhaustive evaluation and findings of the Review Board, is reproduced in-part below.

Electric Arcs: Teflon has excellent fire resistance, but low resistance to cold flow (see "Cold Flow" inset). The Teflon covering on the wire used in Apollo 204 could also be damaged easily or penetrated by abrasion. In addition, the Board found numerous examples in the wiring of poor installation, design, and workmanship. If a power conducting wire experiences penetration of its insulation by the metal structure of the spacecraft or spacecraft components, an instantaneous short to ground is created at the point of conductor contact. An arc or a series of arcs between conductor and structure will result. Circuit breakers and other practical circuit interrupting devices cannot act rapidly enough to prevent an arc. Thus, arcs cannot be eliminated as a potential source of ignition energy. As noted previously, there were strong

Figure 2: Wires where the fire was suspected to have started.

data indications of an abrupt, short-duration voltage decrease. This is consistent with a quickly terminated arc.

Cold Flow: Cold flow (or creep) deformation involves the insulation gradually separating or flowing apart from a pressure point, such as in the case of a foot resting on exposed wire that is held against a metal edged structure.

Underlying Issues

Design & Material Issues

Both wiring and plumbing installation designs were faulted by the accident Review Board – "unprotected vulnerable wiring carrying spacecraft power and vulnerable plumbing carrying a combustible and corrosive coolant." The choice of Teflon as the wire coating may have been a good choice from the standpoint of fire resistance but the wrong choice for wires that were directly exposed to the cabin environment.

The selection of a 100% oxygen atmosphere was made despite the potential hazard. The decision was an accepted risk. The absence of a mature systems safety process was demonstrated by the presence of extensive combustible materials in the cabin, even though the intention to limit such material was the rationale and basis, in-part, for approving the 100% oxygen atmosphere. In addition, the hatch design which opened inward did not provide the means to quickly egress the crew in the event of a fire, as the pressure buildup inside the cabin creates massive forces against opening the door.

Figure 3: Commemorative patch.

Quality Control

Issues concerning NAA personnel management, equipment, parts, procedures, workmanship, and contamination were released to the press in 1966 by KSC quality inspector Thomas Baron in a 55 page report. At the time, NAA analyzed the accusations and denied most of them, although later the company admitted that about half of them were valid. Mr. Baron was called to testify before Congress after the accident.

Emergency Preparedness

The Review Board cited inadequate provisions for emergency response or rescue as a contributing cause. Also, the fire and medical teams were not initially present when the fire started.

Budget and Schedule Pressures

The Apollo 1 fire took place in the charged environment of Cold War national urgency – speed was imperative. In addition, NAA was under intense scrutiny and criticism from NASA over cost overruns and schedule delays in the years prior to the mishap. These concerns led to an investigation by Apollo Program Director Major General Samuel C. Phillips in late 1965. In retrospect, time and budget pressures could be viewed as contributing factors to the design, manufacturing, and quality control process issues noted above.

Aftermath

The Apollo 204 Review Board was established on January 28th and consisted of 10 people, 7 of whom were NASA employees. The analysis ultimately involved 1500 experts in 21 panels investigating different aspects of the accident. The final report of the Board, released April 5th, was 3000 pages long.

NASA aggressively responded to implement the Board's suggestions, switching to "Block II" (upgraded) spacecraft already in development, which included many of the recommendations of the Board, such as better hatch design which would open outwards and be operable in less than 10 seconds. Better fire resistant materials were developed for spacesuits, concerns about a pure oxygen environment for ground tests were addressed, higher quality wiring with abrasion protection and fireproof coatings was used, new emergency procedures and equipment were added, and almost all flammable materials inside the spacecraft were removed. In all, about 1500 changes were made, resulting in a more secure and safer vehicle. In addition, NASA implemented management changes moving astronauts into more management positions and creating an independent flight program office at Headquarters. Space flight centers were tasked to review all aspects of design, manufacturing, test, and flight from a safety standpoint.

Lessons Learned for NASA

The Apollo 1 case study is particularly important for NASA to consider in development of designs for the Orion spacecraft and Ares family of booster rockets. The design tradeoff process must actively engage with the design system safety hazard analysis process to ensure that any mitigation measure or safeguard for a known hazard in the accepted design is indeed implemented and verified with rigor. The Apollo 1 case demonstrates how previous success (over 1000 hours of flight) with a recognized, but not properly mitigated hazardous condition, can lull managers, designers and operators into complacency, believing that a fire is highly unlikely or

that the danger was overstated. Program and project managers, team members, and assurance professionals need to ask every day: have we just been lucky or do we have real margins and real hazard mitigation measures in place?

"In memory of those who made the ultimate sacrifice so others could reach for the stars"

- Apollo 1 Memorial Plaque

The case further underscores the need to understand material properties (e.g. flammability) across the full range of operating environments, in this case a 100% oxygen atmosphere. Understanding consequence, in a risk management context can be an abstract proposition. Many people involved in the Apollo program had no real appreciation for the dangers associated with the 100% oxygen operational environment. More hands-on engagement with hardware and test environments, fire and explosion training, and/or hazard demonstrations will assist designers of space systems to better understand risks.

Another important theme is systems engineering and integrated hazard analysis (one sub-system hazard triggering other sub-system events). Had the wiring designers considered the consequence of a short circuit arc in a 100% oxygen atmosphere with flammable material present, certainly a more robust physical abrasion protection system would have been implemented.

A final topic to consider, and one of the most vexing challenges for the engineering profession, is the responsibility to ensure that the solution to one problem does not become the source of the next. Avoiding this outcome is a principal role of the systems engineering discipline. Consider the inward opening door that mitigated the likelihood of losing the door and swamping the capsule as occurred on the Mercury MR-4 mission. This improved hatch proved an egress liability in the case of the Apollo 1 fire. The second example embedded in this case study is the evolution of wiring in aerospace systems. Recognizing the cold-flow vulnerability of Teflon, Dupont developed an extremely abrasion resistant wire in the late 1960s known as Kapton polyimide (perhaps in part a response to the Apollo 1 fire). While possessing many admirable qualities in terms of durability, Kapton insulated wire proved, over time, to be vulnerable to cracking on tight radius turns and had a hidden and insidious failure mode known as arc-tracking (a current limiting short circuit) which can lead to a catastrophic event known as flash-over. Kapton related failures occurred in both military and civil aerospace applications, most notably TWA Flight 800.

Questions for Discussion

- To what extent is systems engineering emphasized and executed within your program? Who are the leaders in your work group who promote and elevate the systems perspective?
- In engineering tradeoff deliberations, are all risks and/or hazards treated in a balanced fashion? Do certain risk issues have a "louder voice" at the table?
- How do you avoid complacency when you have repeatedly been successful at inherently hazardous or difficult tasks?
- Do you review hazards and critical items in your project or program periodically to ensure that they are still appropriate, correct, and that any controls and other mitigations are properly implemented?

References:

Siddiq, Asifi "Mutual Influences: U.S.S.R.-U.S. Interactions During the Space Race" from Looking Backward, Looking Forward, 40 Years of US Spaceflight Symposium, Edited by Stephen Garber. The NASA History Series, NASA History Office, 2002.

Perrow, Charles, "Normal Accidents", Princeton University Press, Princeton, NJ, 1999.

Lambright, W Henry, "Powering Apollo – James E. Webb of NASA", Johns Hopkins University Press, Baltimore, MD, 1995.

Shayler, David, "Disasters and Accidents in Manned Spaceflight", Praxis Publishing Ltd., Chichester UK, 2000.

Halvorson, Todd, "Making Impossible Possible," Florida Today, January 28, 2007.

Multiple references under "Apollo 1, Apollo 204, Mercury, Gemini" available at NASA web sites within the following domain http://www.hq.nasa.gov/office/pao/History.

SYSTEM FAILURE CASE STUDIES

NSC

NASA SAFETY CENTER

This is an internal NASA safety awareness training document based on information available in the public domain. The findings, proximate causes, and contributing factors identified in this case study do not necessarily represent those of the Agency. Sections of this case study were derived from multiple sources listed under References. *Any misrepresentation or improper use of source material is unintentional.*

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov

National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

NOVEMBER 2008 VOLUME 2 ISSUE 9

The Million Mile Rescue

The Solar Heliospheric Observatory spacecraft (SOHO) is a major element of the joint ESA/NASA International Solar Terrestrial Program. It was launched on December 2, 1995, and successfully completed its primary mission by 1997. After implementation of code modifications meant to increase SOHO's lifetime during its extended operations phase, multiple errors in the new command sequences repeatedly sent the spacecraft into an emergency safe mode. One key error remained undetected while ground controllers made a critical mistake based on an unconfirmed and faulty assumption. SOHO's attitude progressively destabilized until all communication was lost in the early hours of June 25, 1998. It took three months to miraculously recover and restore SOHO to full mission status.

Figure 1: Artist's conception of the SOHO spacecraft.

BACKGROUND

The Solar Heliospheric Observatory (SOHO) is a joint international project between NASA and the European Space Agency (ESA) to study the Sun, from its deep core to the outer corona, and the solar winds, using 12 on-board scientific instruments (Figure 1). Launched on December 2, 1995, SOHO was designed for a two year mission. But in 1997, the mission was extended to 2003 because of its spectacular success. This extension was the basis of the code modification that sparked this mishap. After recovery, subsequent extensions were granted through 2009.

SOHO was designed to revolve around the Sun in lock step with the Earth's own revolution (Figure 2) by maintaining a halo orbit around the First Lagrangian point, where the combined gravity of the Earth and the Sun keep SOHO's orbit anchored in the Earth-Sun line. Once in this orbit, SOHO's attitude was generally stable and used spinning reaction wheels controlled by an Attitude Control Unit (ACU) computer to autonomously adjust for internal or external disturbance torques. If the wheels reached a spin near their design limit, ACU automatically despun the wheels, used thrusters to stabilize attitude, and then reactivated the wheels to resume attitude control. The ACU used a gyroscope (Gyro C) to sense roll attitude during these maneuvers.

SOHO also contained a second gyro (Gyro B), used solely for fault detection (e.g. to sense roll rates beyond some predetermined tolerance). If an excessive roll rate was detected, SOHO was triggered to enter a "safe mode," where it ensured that its panels were facing the Sun, temporarily suspended the ACU computer, and then awaited ground commands. This was called an Emergency Sun Reacquisition (ESR) mode, and it required ground commands to restore normal operations under the ACU. During recovery from an ESR, ground controllers used the third and final gyro (Gyro A), instead of Gyro C, for roll rate sensing. The recovery sequence finished with a recalibration of all three gyros and a restoration of Gyro C to roll rate sensing.

WHAT HAPPENED?

Gyroscope Misconfigurations

Each gyro is used only for its specific independent function. And all three require periodic calibrations to account for drift bias, which is a common result of mechanical wear, angular changes, or exposure to extreme temperatures. The drift bias is determined by ground engineers and is then uplinked to the spacecraft's on-board computer with the correct coordinates for each gyro, allowing the spacecraft's attitude control functions to operate accurately. Due to the same mechanical and thermal wear that causes drift bias, gyros eventually become non-operational, which became a concern as the SOHO mission was extended.

In February 1997, the flight operations team modified gyro command sequences to attempt to address this issue. Specifically, a command was written to deactivate (spin down) Gyro A when not in use, which is any time other than ESR mode. The code was supposed to include a function to re-spin Gyro A upon entering an ESR (a function actually mandated for spacecraft safety). However, this function was erroneously omitted in the new command sequence. The modification had been introduced with a Mission Operations Change Request (MOCR) in March 1997 but was not used in gyro calibrations until June 24, 1998. Therefore, even though the SOHO spacecraft had entered the ESR mode four times prior to June 24, the code modifications were not in use and did not affect successful recoveries by ground crews. But the software modifications also contained a second critical error. The fault detection setting on Gyro B was 20 times more sensitive than it should have been. It was this latter error that triggered this mishap and sent SOHO into its fifth ESR mode (ESR-5) at 7:16 pm on June 24, 1998.

The recovery effort began immediately but was complicated by the aggressive scientific task schedule planned for June 24-29. The core SOHO team was already working on a compressed timeline without the luxury of additional support or contingency time. Ground controllers quickly discovered and corrected the error in Gyro B but did not notice that Gyro A had not reactivated during the ESR. Shortly thereafter, as a normal part of the recovery sequence, all three gyros were recalibrated, and the ACU was activated to make any necessary adjustments using its thrusters. However, when the ACU attempted to correct for the drift bias on the spun down Gyro A, its roll rate reading did not change with thruster firings. The ACU continuously attempted to correct for a perceived (but non-existent) roll attitude error until the actual roll rate increased so significantly that Gyro B's fault detection accurately triggered ESR-6 at 10:35 pm.

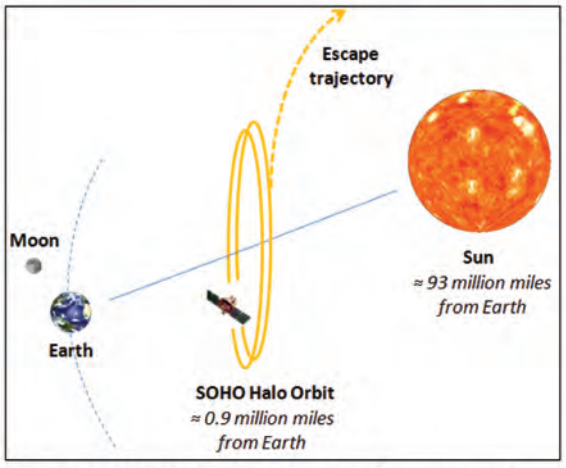


Figure 2: SOHO's halo orbit is about four times the distance away from Earth as the moon. Escape trajectory is also shown. Schematic is not to scale.

Critical Decision Mistake

Again, recovery efforts initiated immediately. It was observed that Gyro B's readings of an excessive roll rate did not agree with Gyro A's nominal reading for the roll rate, but the flight operations crew still failed to notice that Gyro A was not even spinning. Gyro C was not consulted, since it was replaced by Gyro A during ESR. In a rapid decision, the flight operations manager incorrectly concluded that it was Gyro B (and not Gyro A) that was faulty. Gyro B was ordered to be shut down, which also rendered fault detection capability inactive. When control was returned to the ACU for the recalibration sequence of recovery, roll thruster firing resumed and Sun-pointing errors eventually resulted in pitch and yaw thruster firings. This produced unstable spinning of the spacecraft that exceeded allowed limits for a Sun-pointing anomaly and triggered ESR-7 at 12:38 am on June 25. Within minutes, SOHO's attitude diverged beyond control. Power, communications, and telemetry signal were all lost. By 12:43 am, SOHO was officially lost in space.

The Million Mile Rescue

Within hours, investigation teams at both ESA and NASA had been assembled. On June 28 they convened at Goddard Space Flight Center in Greenbelt, MD, to begin recovery efforts. Based on the last few minutes of telemetry, simulations predicted possible trajectories for SOHO indicating that if the spacecraft was not recovered by mid-November, it would diverge and escape into a solar orbit (Figure 2). By a stroke of good fortune, calculations also indicated that in roughly 90 days the spin of the spacecraft would naturally align the solar arrays with the Sun for about half of a spin period, giving the recovery team the opportunity to regain control over SOHO within the time window. On July 23, combining the Arecibo radio telescope in Puerto Rico with NASA's Deep Space Network in California the team was able to locate the spacecraft's radar echoes and confirm both its location and spin rate.

The flight operations team uplinked commands to SOHO for 12 hours a day, searching for any signs of return communication. On August 3, contact was established. Over the next two months, SOHO was progressively restored to normal operating mode. On September 25, about 90 days after contact was initially lost, SOHO was fully operational. Remarkably, all 12 scientific instruments remained in complete working condition despite having been subjected to temperatures from -120 °C to 100 °C during the 3-month ordeal.

Proximate Cause

The SOHO Mission Interruption Joint ESA/NASA Investigation Board determined that the mishap was a direct result of ground operations errors and that there were no anomalies on-board the spacecraft itself. Due to critical software errors in the modified gyro command sequence, SOHO's gyros were configured incorrectly, causing the ACU to erroneously fire its thrusters until the spacecraft destabilized. This was exacerbated by a key decision to shut down a gyro believed to be malfunctioning in favor of a gyro that was actually inactive.

Underlying Issues

Lack of Change Control

Modifications to the command sequences were not properly documented, communicated, reviewed, or approved by either ESA or NASA. The MOCR itself was an internal flight operations document only distributed within the team. The only testing performed was by a NASA computer-based simulator that verified each change separately, but not all together. The investigation board found that there was little done to determine any implications of the changes on overall system reliability. There were no code walk-throughs, no independent reviews, and no hard copies of the command sequences. The filename itself was not updated to reflect that modifications had been made.

"At any time during the ... emergency situation, the verification of the spinning status of Gyro A would have precluded the mishap."

-ESA/NASA Investigation Board

The spin status of the gyros was not obvious to ground controllers and allowed roll rate readings to be collected and misinterpreted, even when the gyro was despun. An effective design would have made it inescapably clear whether or not a gyro was spinning.

Failure to Follow Procedures

The ESR safe mode was designed to give flight operations and engineering teams sufficient time to understand problematic anomalies before taking action. SOHO was programmed to store the last three telemetry frames prior to an ESR so that they would be available for examination by ground crews. The operations procedures specifically stated that before attempting a recovery, Gyro A should be confirmed to be spinning and the last three telemetry frames should be analyzed. The SOHO operations team did not take advantage of this design and instead chose to initiate recovery sequences almost immediately after each ESR was triggered without checking either Gyro A's spin status or the telemetry data. If the spin status of Gyro A had been verified according to proper procedures, the operations team would have known that the destabilizing thruster firings were not due to a faulty Gyro B. When Gyro B was spun down, SOHO lost its autonomous fault detection system. Standard procedures require that such a critical action be approved by a Materials Review Board so as to provide a formal review by senior management and engineers before proceeding; however, no such board was ever convened.

Overly Aggressive Task Scheduling

The scientific activities planned for June 24-29 did not allow for contingency time in the schedule. The flight operations team felt that they did not have adequate time to analyze the results of gyro calibrations. Normally, recalibrated gyros were given 12 hours for verification that the drift biases had been corrected before moving forward. But with SOHO, the operational timeline simulations were being implemented in parallel with performance of the actual timeline. Even as operations continued, scientists were debating discrepancies between the results of ESA and NASA simulations as to the feasibility of the "compressed" timeline. The core SOHO team was expected to perform sufficiently without being augmented by additional staff. However, the board determined that the actual staffing of the project was not commensurate with that originally agreed upon in the ESA/NASA Mission Management Plan. As a result, during the ESRs, key engineers were preparing for upcoming science tasks rather than assisting in the recovery. Recovery efforts were rushed in order to return the spacecraft to performing its science operations as quickly as possible. Ironically, the prioritization of science over spacecraft safety contributed to the loss of science operations for three months and risked the total loss of SOHO.

Inadequate Staffing and Training

The IB stated that the flight operations team had not been provided the necessary training in the details of the SOHO spacecraft design and operations to effectively diagnose and resolve anomalous conditions with the spacecraft. Reasons for this included high turnover of personnel and descoping of roles. For example, the Mission Management Plan required a dedicated NASA project operations director responsible for programmatic matters, overall technical direction to the flight operations team, and interfacing with the ESA technical support manager. This position changed hands five times throughout the mission lifetime (including as recent as three weeks prior to the mishap) and had been descoped to require that only 10% of one NASA individuals' time be dedicated to tracking SOHO operations. Therefore, the flight operations team relied heavily on the only two staff members with comprehensive knowledge of the spacecraft. Unfortunately, neither of these two had any expertise in the programming language used to code the command sequence scripts.

Aftermath

The SOHO Mission Interruption Joint ESA/NASA Investigation Board released its final report one month prior to the full recovery of the SOHO spacecraft, urging that its recommendations be reviewed before the resumption of normal SOHO operations. The Board called for a review of the change control process by both ESA and NASA, as well as an examination of all past changes made since the SOHO launch. The Board also recommended an immediate audit of all on-going ESA/NASA International Solar Terrestrial Program flight operations, including an independent assessment of the NASA SOHO simulator, to be led by ESA. Overall, the Board cited a lack of clear leadership in handling contingency situations concerning the spacecraft's health and safety.

Lessons Learned for NASA

Modifications or updates to procedural scripts should require formal approval before implementation, and the entire script (not just the modification) should be revalidated. Flight critical software must undergo rigorous independent validation and verification. On-off status of equipment should be unmistakably clear.

Operational timelines should be planned and validated before implementation, not in parallel with implementation, with the proper attention and reserve given to contingency planning and safety. Risk-based analyses of operations plans should be performed to determine the appropriate levels of insight and oversight to ensure that risks are adequately recognized and controlled. Tests and simulations should be coordinated as not to conflict with management and operations of real-time, on-orbit events. The health and safety of a spacecraft are critical in achieving any scientific or operational goals.

Staffing levels should be assessed, strengthened as required, and provide the capability for surge support to contingency operations. This can be difficult in extended operations that may have limited budget flexibility. But operations teams must be well trained on the systems they will be required to use and should practice emergency and off-nominal situations. Management should be prepared for team turnover and ensure that all staff has the appropriate knowledge needed for successful operations.

Questions for Discussion

- Are all changes or modifications documented, reviewed, and approved by a clear authority?
- When working with others, do you feel that everyone's roles and responsibilities are clearly delineated? Are staff fully trained?
- Are staffing levels adequate to meet schedule demands without sacrificing formal procedures? Do you have adequate surge support capabilities?
- How are priorities set in contingency situations? Are they risk based? Do they circumvent formal procedures?

References:

ESA Bulletin 97 – SOHO's Recovery – "An Unprecedented Success Story", March 1999, http://sohowww.nascom.nasa.gov/operations/Recovery/vandenbu.pdf

Final Report – Joint NASA/ESA Investigation Board, SOHO Mission Interruption, August 31, 1998, http://umbra.nascom.nasa.gov/soho/SOHO_final_report

NASA Public Lesson Learned 0664, SOHO Mission Interruption, December 01, 1999, http://www.nasa.gov/ offices/oce/llis/0664.html

"Evaluating Accident Models Using Recent Aerospace Accidents" – Nancy Leveson, June 25, 2001, http://csel.eng.ohio-state.edu/woods/accident_reports/NASA/ leveson_soho.pdf

Artist rendition of the SOHO spacecraft [Online Image], http://www.exploratorium.edu/eclipse/cme_images/soho_30x.jpg

SYSTEM FAILURE CASE STUDIES

NASA SAFETY CENTER

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov

National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

JANUARY 2008 VOLUME 2 ISSUE 1

Forrestal In Flames

On July 29, 1967, a tragic string of events culminated in disaster on the flight deck of the USS Forrestal resulting in the deaths of 134 sailors. As twenty-seven fully armed combat aircraft were on deck in preparation for a bombing mission over North Vietnam, a wing mounted Zuni rocket was inadvertently launched from an F-4 Phantom. The rocket flew across the flight deck and penetrated an externally mounted fuel tank of an A-4 Skyhawk, flooding the deck with hundreds of gallons of jet fuel which quickly ignited. The fire engulfed the aircraft and spread quickly, fanned by 32 knot winds. One minute and 34 seconds later, one of that same Skyhawk's 1000 pound bombs "cooked off," with an explosion that sent shrapnel, flame, and destruction across the flight deck, wiping out the fire fighting crew, and wreaked havoc below deck. Over the next hour, eight more 1000 pound bombs exploded, each time taking the lives of another valiant team of sailors fighting the blaze. The ship was able to return to Subic Bay, Philippines, but fires continued below deck for over 24 hours.

Figure 1: Forrestal crew fights to quell the raging jet-fuel fires.

BACKGROUND

The USS Forrestal, christened and launched in Newport News, Virginia in December 1954, was the supercarrier of its time. Forrestal was the first ship designed specifically to handle jet-powered aircraft and incorporated the very best technology of the 1950's.

Captain John Beling, a decorated combat veteran of World War II, took command of Forrestal in May 1966. In June of the following year, Forrestal left Norfolk, Virginia with over 5,000 enlisted men and officers, en-route to an area in the South China Sea, off the coast of North Vietnam, called Yankee Station. This would provide the base of operations for air strikes on targets in North Vietnam. During the voyage, a great deal of attention, drilling, and training was devoted to fire prevention and firefighting. Captain Beling even distributed a "case study" of the 1966 fire aboard the aircraft carrier Oriskany (involving magnesium flares) that took the lives of 44 enlisted men and officers.

Weapons Carrier Design

The triple ejector rack (TER) served as a mechanism to launch rockets mounted in pods underneath the wings of fighter and attack aircraft. The TER was designed with two independent safe and arm systems. First was the "pigtail" plug that had to be in place for electrical signals from the cockpit to reach the launcher element within each TER. Operational procedures stated that "the pigtail connector shall not be plugged in to the receptacle until just before takeoff," typically while seated on the catapult with a clear field of fire. The second safeguard was the TER safety pin (or TER-pin). This pin mechanically opened all firing circuits in the launcher, and procedures called for it to be removed immediately before takeoff. The two-fold safety controls were consistent with standard safety philosophy.

Forrestal In Flames:

134 dead, 161 injured.

Proximate Cause:

- Power Surge in F-4 Phantom triggered lanch of Zuni rocket while Phantom was parked on deck

Underlying Issues:

- Zuni rocket launcher design flaws
- Combat time pressures resulting in waivers and on-the-fly procedural changes
- Miscommunication of and lack of common line involvement in procedural changes
- Dangerously unstable ordnance
- Insufficient firefighting training and infrastructure

Safety Board and Safeguards

On June 29, 1967, on the way to Vietnam, Forrestal's Weapons Coordination Board (WCB) approved a waiver to the requirement concerning pigtail connectors, allowing insertion of the pigtail while the aircraft was parked on the aft flight deck as an operational time saving measure. The WCB logic was that this shortcut was acceptable because the TER-pins were in place until launch. The WCB decision was never forwarded to higher authority for review, as was called for in standard operating procedures.

Additional Time-Saving Initiatives

Unfortunately, flight maintenance crews for certain squadrons, driven by the acknowledged need to save time, had, on their own volition, made similar informal determinations concerning the TER-pin. They reasoned that early removal of the TER-pin would save time and was supported by the logic that the pigtails would not be in place until launch. This breach of process discipline went undetected by first-line supervisors at the time.

"Every sailor (must be) a firefighter. Every engineer, a safety engineer."

Ordnance Supply and Management

On the evening of Friday, July 28, 1967 the Forrestal accepted a load of dangerous 1000 pound "B"-bombs, some manufactured as early as 1935, rusty, poorly stored and maintained, and notoriously sensitive to heat and impact. The Forrestal was used to using the newer H-6 model, designed to withstand high heat and vibration. Captain Beling had protested but was told that no alternative ordnance was available. It was the B-bombs or nothing. Pressed to launch air strikes the next morning as part of the major US air offensive, the Captain reluctantly accepted the weapons.

What Happened?

The next morning, the Forrestal launched the first strike of 37 aircraft between 7:00 am and 7:50 am. The strike force returned by mid morning. and the deck was reconfigured for the second strike, scheduled for 11:00 am.

By 10:51 am, all of the 27 aircraft assigned to the strike were manned and engaged in pre-flight checks, with some beginning to start their engines. Pilot Jim Bangert was in the cockpit of his F-4 Phantom. He had started his starboard engine providing internal power and was prepared to switch from the tractor external power supply. His ground crew had just connected the pigtails in accordance with the waiver procedures (and under the assumption the TER-pin was still in), effectively arming the six and-a-half foot long, five inch diameter Zuni rockets.

At 10:51:21, he hit the power cutover switch, and one of his Zuni rockets blazed across the deck, chest high, severely burning members of Bangert's ground crew, severing a man's arm on its way across the deck and ripping open a loaded fuel tank of an A-4 Skyhawk (piloted by John McCain, now US Senator from Arizona). Hundreds of gallons of JP-5 fuel spewed onto the flight deck and ignited directly beneath the wing mounted 1000 pound B-bomb payload. One minute and 34 seconds later, the B-bomb exploded.

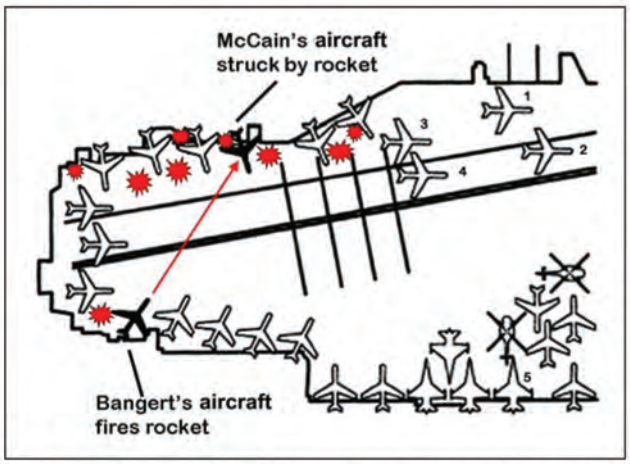


Figure 2: Arrangement of aircraft at time of the rocket misfire.

The initial blast killed five of the eight members of Damage Control Team #8, specifically trained for flight deck firefighting. The other three were severely injured. Twenty-two others died in the initial blast. Lt. McCain had successfully egressed his burning aircraft and was en-route to the island when the bomb went off. He was hit by several pieces of shrapnel, but his wounds were minor. In the next half hour, eight more 1000 pound B-bombs exploded with horrific effect. Before the fires were under control, a total of 134 men were killed and 161 injured. Over 20 aircraft were lost.

Proximate Cause

Attempting to change-over his F-4 Phantom to internal power, Pilot Jim Bangert hit the power cutover switch which, due to an electrical relay design deficiency, initiated a power surge to his Zuni rocket launcher. Independently and without each other's knowledge, the WCB and maintenance crews had compromised both redundant ordnance launch prevention systems – connection of the pigtail and removal of the TER-pin – by performing those functions significantly before take-off, allowing the not-uncommon power surge to cause the Zuni rocket to fire.

Underlying Issues

This system failure was the result of multiple factors which included design deficiencies (frequent and unexplained power-on surge during aircraft change-over from a start-up power cart to internal power), intentional and unintentional lowering of safety barriers, unrecognized lapse in process discipline, and hazardous ordnance.

Zuni Launcher Design Issues

Captain Beling questioned the intrinsic design safety of the LAU-10 safety and ignition system (which included the pigtail and TER-pin). His testimony before the investigation board stated, "It is evident that Forrestal's ordnance personnel never had a safe system to work with and never had the technical information needed to design prudent, sailor-proof rocket loading and arming procedures." It was noted that only two months earlier (May 1967) a Zuni rocket misfired from an F-8A Crusader sitting on the deck of the carrier Hancock. Fortunately, the rocket missed personnel and other aircraft; the exact cause of the misfire is still unknown.

Operational Time Pressures Driving Official and Unofficial Changes in Safety Procedures

The official WCB decision to allow early insertion of pigtails to save time in an operational war fighting scenario removed the first critical barrier to disaster. The unofficial practice of removing TER-pins prior to the last minute effectively removed the second critical safety barrier. First line supervisors with certain squadrons were either unaware or participating in practices which deviated from safety requirements, specifically, removing TER-pins prior to take-off position.

Safety Management Communication & Leadership

The lack of line management (command) visibility into and involvement with the WCB process as well as oversight of operational crew practices was also a contributing factor. The accountability concern extends to all management levels within both sea and air wing chains of command.

Hazardous Ordnance

The time pressures to support the 1967 air offensive coupled with logistical supply issues resulted in Navy upper management decisions to use obsolete weapons that had been stored in open-air sheds in the Philippines since the end of World War II. Some of the bombs were in crates labeled 1935.

Inadequate Firefighter Training, Infrastructure & Equipment

Despite Captain Beling's efforts to accelerate fire-fighting training in the year before deployment, many of the crew remained untrained, especially in jet-fuel fires. With Damage Control Team #8 decimated, untrained sailors valiantly fought jet-fuel fires with water hoses (the wrong thing to do) rather than foam. Only half the ship's crew and none of the Air Wing crew had attended firefighting school in the previous three-year period. In addition, Air Wing sailors (40% of the Forrestal crew) were not trained to use an oxygen breathing apparatus and were not well oriented to Forrestal damage control processes and equipment. Numerous problems were also identified related to flight deck "foam station," design, operational readiness and training for foam station operators.

"Half the ship's crew and none of the Air Wing crew had attended fire-fighting school."

Aftermath

The investigation board chaired by Admiral Massey issued a 7,500 page report which concluded that "the deaths and injuries resulting from the fire aboard the Forrestal on July 29, 1967 were caused by the negligence and inefficiency of the Headquarters, Naval Air Systems Command." At the same time, the report provided over 30 findings and recommendations addressing shortfalls in damage control process design and damage control equipment, as well as poor training and execution of damage control functions. The Chief of Naval Operations, Admiral Moorer, empanelled a follow up investigation into Navy-wide aircraft carrier safety led by retired Admiral James Russell that concurred with the Massey report, as well as citing the need for better personal protective equipment.

Applicability to NASA

The belief in a redundant system that is in actuality compromised or ineffective is a tragic lesson that NASA learned during the Space Shuttle Challenger mishap. All can benefit from a reminder to never remove a safety critical barrier in a high-consequence environment without a full understanding of the status of remaining controls. Operating with one safeguard requires careful deliberation and approval by accountable management at appropriate levels as well as verification that the secondary barrier is, in fact, effective and has been implemented.

Another important thematic lesson involves the need to elevate safety critical waivers, deviations, or exceptions to senior management levels within organizations potentially aff-

Figure 3: The crew continue to fight the blaze that killed 134 sailors

ected by the departure from requirements. That is, leadership and management must implement processes that ensure their ongoing and real-time knowledge, understanding, and visibility into critical details of hazardous activities and operations.

Figure 4: USS Forrestal in action.

Design and test project teams are reminded of the need to understand hardware/software electro-mechanical system behavior in off-nominal and transient upset environments. The power change-over, believed to have been an initiating event, clearly was an operating environment in which the LAU-10 system should have been design-hardened to withstand power-on transients and verified through extensive testing. Understanding material properties, detonation hazards, and shelf-life characteristics is underscored by the use of B-bombs with unknown (only anecdotal) properties, manufacturing and storage history. The case further instructs teams to maintain focus on configuration management and record keeping for pyrotechnics, propellants, batteries, pressure vessels, and other hazardous materials and systems. What are the shelf-life constraints? Does the hazard risk increase with time? Communication, training, and safety leadership are also resonant themes for NASA.

Questions for Discussion

- Why was the Zuni rocket launch system not immediately placed in a "hold – do not use status" until the May 1967 Hancock inadvertent firing was understood and corrected? Was it the demands and/or constraints of the war? Or failure to fully understand the consequences?
- What approaches are you using to verify hazard controls in safety critical systems you employ? How do you ensure reliance on redundant systems doesn't cause complacency?
- How can NASA prevent the evolution of "informal waivering" of safety requirements in the interest of expediency?
- Any waiver, even an official waiver, can increase risk. What steps does your group take to understand and mitigate risks resulting from requirement waivers? Are these waivers and their acceptance rationale revisited on a routine basis?

REFERENCES:

Freeman, Gregory A., "Sailors to the End," Morrow Publishing, 2002

Stewart, Henry, P., "The Impact of the USS Forrestal's 1967 Fire on United States Navy Shipboard Damage Control," U.S. Army Command and General Staff College, Master Thesis, Fort Leavenworth, Kansas, 2004, WWW site accessed July 2007, http://www.stormingmedia.us/30/3019/A301924.html.

National Public Radio interview, Scott Simon's interview with Gregory A. Freeman, August 2002, WWW site accessed July 2007, http://www.npr.org/programs/wesat/features/2002/aug/ussforrestal/index.html.

Bill Thompson, Eye on Books ,interview with Gregory Freeman, August 2002, WWW site accessed July 2007, http://www.eyeonbooks.com/nonfiction4x.html.

SYSTEM FAILURE CASE STUDIES

NSC

NASA SAFETY CENTER

This is an internal NASA safety awareness training document based on information available in the public domain. The findings, proximate causes, and contributing factors identified in this case study do not necessarily represent those of the Agency. Sections of this case study were derived from multiple sources listed under References. *Any misrepresentation or improper use of source material is unintentional.*

To view this document online and/or to find additional System Failure Case Studies, go to http://pbma.nasa.gov

Cases of INTEREST

NASA SAFETY CENTER

Cases of Interest (COI) focus on common, Agency-wide hazards or concerns. While each COI features a specific NASA mishap or close call, these incidents represent mishaps Safety & Mission Assurance professionals see again and again in different situations throughout their careers. A COI uses the story of one incident to increase awareness of a greater problem, present potential solutions, and spark conversations on how to make NASA operations safer and more effective.

The COIs in this book are also available online, where they link to related resources. Readers can review NASA requirements and industry standards, catch up on lessons learned, register for relevant training, and access other information tied to the featured incident. These resources help participants understand why the hazard is a concern and how to safely deal with the situation.

COIs can be read by individuals, or they can provide the basis for a group discussion on the COI topic. They are self-contained and do not require outside experts to facilitate discussion or explain nuances of the featured incident; frequently, they include talking points and discussion questions to help begin the conversation.

National Aeronautics and Space Administration

NASA SAFETY CENTER CASE OF INTEREST
11/30/2008

CAN'T GET THERE FROM HERE

Access Control

Primary Case

In a recent incident at a NASA Center, high pressure component testing was being performed in a test cell. Although there were several access controls and warnings in place, unauthorized employees breached the controlled area on multiple occasions during the test.

Access control is often thought of as a tool for security and protecting sensitive information, but this incident illustrates access control's role in ensuring the safety of personnel and equipment during hazardous operations. No one was injured in this close call, but the incident highlights common access control failures that could result in serious injury or damage.

The following list describes some of the reasons multiple employees entered the controlled area during testing:

- The test cell signage was inadequate
- Some of the warning lights were not working
- Reaching into an 'exit only' gate to bypass the locking mechanism and gain entry was routine practice
- The same gate's spring mechanism was broken, so it did not swing shut after opening
- The test cell door was left open under the assumption that the 'exit only' gate prevented access
- Although a warning light was flashing, the open gate and open door indicated the test was over to an employee entering the area
- Misunderstanding of procedure and failure to correct one employee in the past led personnel to believe that the warning lights did not bar entry into the control room

When people and property are at risk, access control is essential. If control measures are not functioning properly, alternative methods of access control must be implemented before beginning operations.

Barrier design must be effective for personnel who may not have been trained and for those who may not follow procedure. Individuals should not be able to bypass or override essential access controls. Use administrative controls such as lights, signs or caution tape to supplement—not replace—physical access barriers.

This incident initiated several design and procedural changes to address the multiple failures that occurred. These changes reduce the likelihood of recurrence of a similar incident.

NASA SAFETY CENTER CASE OF INTEREST
11/30/2008

CAN'T GET THERE FROM HERE
Access Control

Agency Status

While most Agency-wide guidance specific to access control relates to securing information, NPR 1620.3 "Physical Security for NASA Facilities" gives guidance for restricting access to certain types of facilities, including research facilities. Also, barricading and access control are addressed in individual documents such as NASA-STD-8719.9 "NASA Standard for Lifting Devices and Equipment." In general, these requirements leave it up to the user to determine appropriate access control techniques that will ensure the safety and health of personnel.

Priority must be given to design of physical barriers and engineering methods that control access, rather than relying on administrative controls. However, in some cases access control will depend on cooperation from employees and contractors. Work with personnel who may be in the area to ensure that individuals are committed to following applicable procedures.

All NASA employees and contractors should work closely with their Center's safety and security organizations to develop effective access control plans.

General Guidelines and Discussion Points

This close call suggests several principles of access control that should help prevent similar accidents during the course of your work:

1. **Avoid assumptions:** In this incident, operators assumed the area was secure, and personnel assumed the open doors indicated the test was over. What assumptions do you make related to access control?
2. **Be consistent:** Employees were repeatedly allowed to ignore warning lights and enter the area during testing. Do you make it a point not to cross hazard barriers? This sets a good example and conditions you to pay attention to access controls.
3. **Use appropriate indicators:** Here, multiple warning lights were not working and signage was not specific. Is your signage clear and complete? Are your indicators in working order?

Protect People and Property from Unauthorized Access

There are many methods of access control. One example of a physical control method is a keyed interlock system that is designed to prevent operator error. Such a system uses multiple keys in a specific, predetermined scheme to ensure proper sequence of operations or entry to an area. In complex facilities and equipment where personnel or property may be at risk, these systems can force operators to perform steps in a safe and logical manner that includes physical checks of the system.

Everyone's Responsibility:

If you observe someone bypassing an access control measure such as a barricade, take the following action:

1. Ensure they are aware of the access control, inform them of the reason for the control, and ask that the person not bypass the control or barricade.
2. Report the incident along with the person's name (if known) to allow for necessary follow-up or training.
3. If immediate action appears necessary to avoid imminent danger, contact emergency personnel.

Any questions regarding access control or barricading should be referred to your Center's safety organization.

Access Control Guides

There are many manuals available for access control, including:

- Manual on Uniform Traffic Control Devices – Part IV
- Chapter 29 – Glenn Safety Manual – Safety Barricades

Training Available at NASA

Training available for access control:

- Signs, Signals, and Barricades - SMA-SAFE-NSTC-0061
- Scaffold Users Seminar - SMA-SAFE-NSTC-0316
- Scaffolding Safety - SMA-SAFE-NSTC-0312
- MSFC Hazard, Identification, and Warning System - MSFC-009-05
- World of Electronic Access Control Sub course 1 – Access Control Components

National Aeronautics and Space Administration

NASA SAFETY CENTER CASE OF INTEREST
8/27/2008

Ghost in the Machine
RF-Controlled Crane Safety

Primary Case

In May 2007, a Radio Frequency-controlled crane at a NASA Center began lifting an object on its own. The key was not turned on; no one was at the controls. Although operators soon regained control of the errant crane, this was a close call that could easily have resulted in equipment damage or severe injury.

This close call represents a hidden hazard in crane operation: RF frequency "Cross-Talk." In this incident, RF emissions from another crane caused the uncommanded movement. It is important to recognize that any emitter of the same frequency and sufficient power—even some handheld radios—within range of the affected crane would have posed a similar risk.

As a result of this incident, a program was established at the center to insure all radio controlled cranes' operating frequencies have sufficient frequency separation to avoid "Cross Talk" between cranes. As part of this program, a list of radio frequencies used to control cranes and other devices will be maintained and shared with appropriate personnel.

Getting Rid of the Ghost

Whenever periodic surveys identify emitters that can interfere with equipment operation or cause hazardous personnel exposure, look for an engineering alternative. This solution might include shielding, alternate frequencies, or reduced power output. If an engineering alternative is not feasible, establish a plan of operation that allows emitter use while mitigating hazardous effects. Normally, such a plan creates separation between the emitter and the undesired target.

Centers are encouraged to check similar cranes to assure their signals/radio frequencies do not overlap. In addition, remember that there are many other devices which could cause "Cross-Talk." If portable devices could interfere with equipment, appropriate signage should be posted to keep the area clear of interfering signals.

** **ISS airlock construction at MSFC:** A properly operated crane lifts the airlock for the International Space Station during construction in the Space Station Manufacturing Building at NASA's Marshall Space Flight Center in Huntsville, Ala. This crane was not involved in the primary case discussed above.*

NASA SAFETY CENTER CASE OF INTEREST
8/27/2008

Ghost in the Machine
RF-Controlled Crane Safety

Background

NASA operates every kind of crane and lifting device to execute its mission. The safe operation of cranes and lifting devices becomes even more crucial as the Agency manufactures and tests new types of flight hardware. To meet manufacturing and assembly needs of this new hardware, Centers are modifying cranes and lifting devices or installing new ones. One concern associated with these changes is the effect that changing a system has on other systems. As illustrated by our primary case, system configuration control and awareness of interface hazards are critical to the safe operations of our facilities. While the featured close call speaks to a specific type of hazard, crane operations present a wide variety of hazards that users and safety professionals must work together to control.

Talking Points

Each Center is required to designate a qualified Center Spectrum Manager to manage all aspects of RF utilization. Each Center is also required to designate a Lifting Devices and Equipment Manager (LDEM) who is responsible for overall management of the Center lifting devices and equipment program. If you have any questions regarding the safe operation of cranes, please contact these designees at your Center. Here are some questions you may want to ask in any discussions regarding cranes at your location:

- Have all of our cranes and lifting devices been tested and managed per NASA-STD-8719.9?
- Have all of our crane and lifting device operators been certified per NASA-STD-8719.9?
- Have we had any incidents of uncommanded crane movement?
- Do we have an inventory of RF-controlled cranes or other equipment?
- Have we made any changes to facilities involving RF-controlled equipment which could impact existing operations?

Related Cases

There have been several recent incidents involving cranes at NASA. While the primary case involved uncommanded crane movement, other mishaps involving cranes are worth mentioning, so that the NASA community can learn from them and avoid similar incidents.

- During a lift operation, a horizontal lifting ring bolt certified for 1800 lbs sheared off when lifting a steel plate (approx. 2000 lbs). [IRIS Case #2007-163-00001]
- A vendor was performing demolition in a building using the facility 10 ton overhead crane. A tank was being lifted and it struck a nearby conduit and broke the conduit. [IRIS Case #2006-310-00005]
- During telescoping crane boom operations, the whip line/headache ball was pulled into the sleeve and disengaged from a single wire haul line and fell to the ground near personnel. [IRIS Case #2007-213-00011]

For more information on mishaps at NASA, please visit the Incident Reporting Information System

Standards

Requirements and guidelines for the safe operation of cranes and lifting devices:

- NASA-STD-8719.9 Standard for Lifting Devices and Equipment
- Occupational Safety and Health Standard, 29 CFR 1910.179, Overhead and Gantry Cranes
- Occupational Safety and Health Standard, 29 CFR 1910.184, Slings
- ASME B30.17, Overhead and Gantry Cranes

Supporting Documentation

Additional information on Radio Frequency hazards and approaches to their control:

- NPR 2570.1 NASA Radio Frequency (RF) Spectrum Management Manual
- IEEE Recommended Practice for Radio Frequency Safety Programs, 3 kHz to 300 GHz
- Radio-Frequency Energy - Hazards & Safeguards
- Naval Safety Center website discussion on Radio Frequency Radiation Hazards
- NASA NPD 2570.5D NASA Electromagnetic (EM) Spectrum Management

Training

Training available for working with cranes and lifting devices:

- Overhead Cranes and Material Handling (SMA-SAFE-NSTC-0205)
- Safety of Mobile Cranes, Derricks, Hoists, Elevators, and Conveyors in Construction (SMA-SAFE-NSTC-0059)
- Cranes and Rigging Safety for Construction (OSHA 2050)
- Crane Operations and Rigging Safety Refresher (SMA-SAFE-NSTC-0028)
- RF and Wireless Made Simple (GRC-3Q1356)

Creating Case Studies in NASA Project Management

A METHODOLOGY FOR CASE WRITING AND IMPLEMENTATION

This overview describes how NASA project case studies are developed and implemented by the Office of the Chief Knowledge Officer (OCKO) at Goddard Space Flight Center (GSFC). The rationale for case-based learning is that knowledge is most usable when it is shared among organization members and when it is contextual—that is, when it relates to one's own experience. Decision-based case studies, such as those developed at Goddard, are structured and written from the viewpoint of a key player, the protagonist. The OCKO takes a 10-step approach to case writing and publishing, as described, briefly, below. The complete case methodology is available on the OCKO Web site, http://www.nasa.gov/centers/goddard/about/organizations/OCKO/.

Step One: Pick a Target

When seeking a subject for a case, look for a topic that needs to be addressed, an experience that has presented itself, a key player in a project or mission who is willing to tell his or her story, or all of the above. Subjects that make for compelling cases include well-known mission or project failures or successes; close calls, incidents, and "lucky" outcomes; and personal insights related to leadership and/or management of current tough decisions.

Step Two: Define the Parameters of the Case

The success of the story depends on the writer staying focused on the learning objectives of the case study. This is achieved by "bounding" the case, or defining the parameters of the story. The most important guideline is to identify learning objectives, the events and persons to be included, and the teaching points to be emphasized.

Step Three: Do the Homework: Background Research

Before talking to the principals involved in the project, gather as much background information as possible. Access public information and collect data from historical and/or current project materials, briefings, and documents, such as reports by the NASA Mishap Investigation Board (MIB). Identify the key decision-makers—they are the primary sources of information.

Step Four: Interview Key Players to Get Their Story

Without direct, open participation by protagonists in constructing the narrative, not only will critical perspectives and information be missing, the story will lack the color and depth only firsthand accounts and quotes can provide. Also, more than one side of the story should be collected. Interviewees might include program and/or project managers, principal investigators, contractors, chief/project scientists or engineers, and other personnel from the project lead center, team members from other NASA centers, and academic and foreign partners.

Step Five: Evaluate Story Lines for Learning Points

At this point, a reality check is in order—now is a good time to consult with the sponsor (at Goddard, the OCKO) of the case-writing effort to review the story line and teaching objectives. This will make it easier to zero in on exactly what story people are willing to tell and how the story can be presented, with implications for the final case study and its likely use.

Step Six: Draft the Case into a Narrative

While writing, keep two principles in mind:

1. Get the story right. This is critical for believability and buy-in.

2. Make the story compelling. This is essential for drawing in participants and keeping them engaged—it addresses the "so what?" criterion.

Beginning: Setting the Context

The case study typically begins with a scenario that frames the issue (or issues) facing the decision-maker as described from his or her point of view. This introduces both the topic and the protagonist(s) as well as the central issues of the case, typically in less than a page.

Middle: Fleshing Out the Story

With the scenario in place—framing the issues and foreshadowing the decisions ahead—the case writer now tells the "back-story," building a narrative that ultimately will return to the time and place at which the case began. The history of the problem is described first, in a project or mission background section, including scientific and mission/project-specific data and historical facts. This is the place for a generous supply of quotations from any primary sources, most importantly (but not only) the key player(s).

Ending: Back to the Beginning

The case now returns to the problem depicted in the opening scenario; by this point, the reader should be able to conduct an analysis for the discussion or decision part of the case. This final section presents a recap of the situation and a recreation of the decision scenario that was established at the beginning of the story. It concludes with a set of questions requiring participants to make decision choices and to consider the potential outcomes of their decisions.

Finalizing the Draft

Once the draft is in a complete narrative form, copy-editing should be done and any missing pieces, such as source attribution of images, should be added. The case should be formatted into standard layout, and graph/chart/table titles should be checked for consistency. While the case will continue to evolve as it is revised, it is important have a well-written and cleanly edited draft ready for review by stakeholders. Stakeholders who will be reviewing the draft should not be expected to read multiple revisions—the content of the story should now be ready for sign-off.

Step Seven: Circulate the Draft

The draft should be stamped "For Internal Use Only" and provided to anyone you may have agreed to allow review the case before publication, by people you think could provide valuable criticism, and/or by anyone whose signoff is required for case to be published.

Step Eight: Test the Case with a Local Audience

The case study should be tested with a low-risk audience before it is put into practice. This may take place in in-house training courses, on team retreats, or in focus groups. These test runs provide important information, insight, and feedback for the final revision and tune-up prior to implementing the case as part of a course curriculum or workshop agenda. The writer should be present to see how the case is perceived (and received) by the audience. This is essential to fine-tuning the case study before finalization and publication.

Step Nine: Create a Teaching Note and an Epilogue

Two accompanying pieces are integral to a complete case study: 1) an epilogue of "what happened," which provides closure to the story to date, and 2) a teaching note. The epilogue is written with information gathered during research, interview material not used in the case, and any relevant information that may have become available since the project concluded. The teaching note is a guide for case instructors. It presents the views of the facilitator (and/or case protagonist) on how the case can be taught most successfully, with an emphasis on conveying the learning objectives. Creating an effective teaching note requires that the writer observe the case being put into practice to see first-hand what works and to witness participants' responses.

Step Ten: Validate, Publish, and Roll out the Case

The case study must be officially authorized before it can be made publicly available. Validation includes making sure all the individuals mentioned in the case study have had a chance to get their story heard; this requires that everyone in the story be involved, to the extent possible, in the case-study process. GSFC case studies are copyrighted with rights to government usage granted; be sure to check with your legal department to follow all its guidelines for public release and copyright procedures. GSFC case studies also carry a disclaimer at the bottom of the first page. After the case has been validated, copyrighted, and approved for release, it is ready for roll-out. At GSFC, this process is initiated by publishing the case and ancillary materials (primarily the teaching note and epilogue) to the Goddard Case Study Library. The case study may then be put to use in any number of forums.

The NASA Story Is Unique—and Powerful

Told the right way—accurately, vividly, with clearly defined learning objectives—a NASA case study has the potential to influence mission success and to help fulfill the NASA mandate to educate and share all that we learn in an open way. In addition to the tremendous science discoveries NASA makes, there is much to learn from how the agency works. In creating and implementing case studies, the most important thing to remember is that we learn from experience, and that all learning leads to a positive outcome.

The Contributors

NASA SAFETY CENTER

The NASA Safety Center (NSC) was established in 2006 to support the safety and mission assurance requirements of NASA's portfolio of programs and projects. Focusing on developing the tools, processes and personnel needed for the safe and successful achievement of NASA's strategic goals, the NSC is comprised of four functional offices: Technical Excellence, Knowledge Management, Audits & Assessments and Mishap Investigation Support.

The NSC's mission is to provide world class support to NASA mishap prevention by:

- Establishing a learning environment; benchmarking from the best and bringing their best practices into our workplace; and learning from our mishaps.
- Ensuring that we are informed risk takers, managing the routine risks in the workplace effectively, and preserving our resources for the execution of the NASA mission.

The NSC case studies in this collection are a joint product of the Knowledge Management and Mishap Investigation Support Offices at the NSC. They are published monthly on the NSC's NASA-only Web site, *http://nsc.nasa.gov*.

For more information, email your questions or comments to *nasa-nsc@nasa.gov*.

GSFC OFFICE OF THE CHIEF KNOWLEDGE OFFICER (OCKO)

The OCKO is responsible for ensuring that GSFC operates as a learning organization. It is responsible for policy and guidance on lessons learned, knowledge management, and learning practices.

The OCKO provides the Goddard Space Flight Center with knowledge management services and support, such as:

- Managing the center lessons learned processes,
- Facilitating the reapplication of knowledge across projects, and
- Enhancing Goddard's development as a learning organization.

The core OCKO activities include:

- Pause and learn (PaL) sessions, which are facilitated team meetings used to transfer individual lessons about a specific project event.
- Case studies, which are produced by the OCKO and used to enhance the participant's learning in the context of Knowledge Sharing Workshops, the RTMS workshop series and in Agency training events.
- Knowledge Sharing Workshops, which provide discussion forums on relevant topics or recently launched Goddard Missions.
- The Road to Mission Success (RTMS) workshop series, which gives upcoming Goddard leaders an integrated perspective on mission success, from procurement and administration to science and mission operations.

The OCKO is led by Dr. Edward W. Rogers, Goddard's Chief Knowledge Officer. Other team members include:

Marisa Connell	Bud Hay	Christopher Reese
Barbara Fillip	John Milam	Charles Tucker
Mark Gatlin	Sumita Nair	Catherine Wiese

More information about the OCKO can be found at the website:
http://www.nasa.gov/centers/goddard/about/organizations/OCKO/

Office of the Chief Knowledge Officer
NASA - Goddard Space Flight Center
Greenbelt, MD 20771 . 301 286 4467

Resources

NASA Safety Center

http://nsc.nasa.gov (NASA only)

http://pbma.nasa.gov

- System Failure Case Studies
- Cases of Interest

GSFC OCKO Website

http://www.nasa.gov/centers/goddard/about/organizations/OCKO/

- Decision-Oriented Case Studies
- Case Epilogues
- Teaching Notes
- Case Methodology

NASA Engineering Safety Center (NESC)

http://www.nasa.gov/offices/nesc/ (NASA only)

- Case Studies and Video Courses

NASA Academy of Program/ Project & Engineering Leadership (APPEL)

http://appel.nasa.gov/knowledge/

- Case Studies
- ASK Magazine Articles and Interviews

Air Force Center for Lessons Learned

http://www.afit.edu/cse/cases.cfm

- Case Studies (full-length report format)

National Aeronautics and Space Administration

NASA Safety Center
22800 Cedar Point Rd.
Cleveland, OH 44142
http://nsc.nasa.gov

www.nasa.gov

NP-2009-02-008-GRC